PHILLIPE DAUTRO DOS SANTOS

CIBERESPAÇO COMO DOMÍNIO DE OPERAÇÕES MILITARES: A PERSPECTIVA DOS ESTADOS UNIDOS DA AMÉRICA

João Pessoa

2018

UNIVERSIDADE FEDERAL DA PARAÍBA

CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS

CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

PHILLIPE DAUTRO DOS SANTOS

CIBERESPAÇO COMO DOMÍNIO DE OPERAÇÕES MILITARES: A PERSPECTIVA DOS ESTADOS UNIDOS DA AMÉRICA

Trabalho de Conclusão de Curso apresentado como requisito parcial para a conclusão do Curso de Graduação em Relações Internacionais da Universidade Federal da Paraíba.

Orientador: Prof. Dr. Augusto Wagner Menezes Júnior.

João Pessoa

2018

Catalogação na publicação
Seção de Catalogação e Classificação

S237c Santos, Phillipe Dautro Dos.
Ciberespaço como domínio de operações militares: a perspectiva dos Estados Unidos da América / Phillipe Dautro Dos Santos. – João Pessoa, 2018.
79 f. : il.

Orientação: Augusto Wagner Menezes Teixeira Júnior.
Monografia (Graduação) – UFPB/CCSA.

1. Ciberespaço. 2. Estados Unidos. 3. Guerra Cibernética. 4. USCYBERCOM. 5. Segurança Cibernética. I. Júnior, Augusto Wagner Menezes Teixeira. II. Título.

UFPB/BC

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
COORDENAÇÃO DO CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

A Comissão Examinadora, abaixo assinada, aprova, com nota 9.0, o Trabalho de Conclusão de Curso

"Ciberespaço como domínio de operações: a perspectiva dos EUA"

Elaborado por

Phillipe Dautro dos Santos

Como requisito parcial para a obtenção do grau de

Bacharel em Relações Internacionais.

COMISSÃO EXAMINADORA

Prof. Augusto Wagner Menezes Teixeira Junior – UFPB (Orientador)

Prof. Gills Vilar Lopes – UNIR

Prof. Alexandre César Cunha Leite - UEPB

João Pessoa, 14 de junho de 2018.

RESUMO

Este trabalho tem como objetivo apontar como a inserção do ciberespaço em políticas nacionais de segurança e defesa tem se mostrado cada vez mais presente nos Estados, em especial nos Estados Unidos da América (EUA). Desse modo, é importante ressaltar o empenho dos EUA na adoção de políticas relacionadas ao desenvolvimento de capacidades operacionais cibernéticas, tanto de forma ofensiva como defensiva, pois a ascensão de adversários no cenário internacional tem representado uma ameaça às suas informações militares-estratégicas, econômicas e políticas. Com o crescente o uso da informação e o desenvolvimento de novas tecnologias, a capacidade de fazer guerra tem ganhado um novo e complexo domínio operacional.

Palavras-chave: Ciberespaço. Estados Unidos. Guerra Cibernética. USCYBERCOM. Segurança Cibernética

ABSTRACT

This work intends to highlight how the insertion of cyberspace into national security and defense policies has been present among countries, especially in the United States. Thus, it is important to emphasize the commitment of the US in adopting policies related to the development of cybernetic operational capacities, both in an offensive and defensive way. The rise of opponents in the international scenario has posed a threat to its military-strategic, economic and political information. With the advent of a new-found use of data and the development of new technologies, the capacity of generating wars has gained a complex operational domain

Key Words: Cyberspace. United States. Cyber War. USSCYBERCOM. Cybersecurity.

SUMÁRIO

À minha mãe, de todo coração.

AGRADECIMENTOS

Dedico este trabalho primeiramente a Deus, pela força e coragem durante essa dura caminhada. Diante dos desafios impostos pensei em várias vezes em desistir, mas refleti, e pedi luz no meu caminho. Muito obrigado.

A minha vó e meu pai, “In Memorian”, que foram importantes na formação do meu caráter e sempre ressaltaram a importância da educação. Agradeço também a minha mãe, por ter sido perseverante comigo e ter dado suporte essencial todos esses anos. A minha irmã que sempre me deu força nas ocasiões mais difíceis.

Agradeço ao meu orientador Augusto Teixeira pela paciência e disponibilidade na realização desse trabalho. Quero expressar agradecimento ao professor Gills, que despertou a temática de assuntos relacionados à área cibernética durante minha graduação.

Além disso, queria agradecer a lealdade e amizade das minhas amigas Andreza Guimarães, Jennifer Maciel, Thalita Lucena e Thays Gomes que foram extraordinárias durante todo o curso de Relações Internacionais.

LISTA DE ABREVIATURAS E SIGLAS

AFCYBER - Comando de Força Aérea Cibernética

AFSCPC - Comandante do Comando Espacial da Força Aérea

ANWB - Batalhão de Guerra de Rede do Exército

ARCYBER - Comando Cibernético do Exército

ASCC – Comando de Componentes do Serviço do Exército

C³I - Comando, Controle, Comunicação e Inteligência

C4I - Comunicações, Computadores e Inteligência

C4ISR – Controle, Comando, Comunicações, Inteligência, Vigilância e Reconhecimento

CDRUSCYBERCOM - Comando Cibernético dos EUA

CEI - Comunidade de Estados Independentes

CMF - Força Missão Cibernética

CNA - Ataque de Redes de Computadores

CNE - Exploração de Redes de Computadores

COMMARFORCYBERCOM - Comando do Ciberespaço das Forças do Corpo de Fuzileiros Navais

CSS – Serviço de Segurança Central

DARPA - *Defense Advanced Research Projects Agency*

DCO - Operações do Ciberespaço Defensivo do Corpo de Fuzileiros Navais

DDoS - Ataque Distribuído de Negação de Serviço

DNS - Sistema de Nomes de Domínios

DoD - Departamento de Defesa

DODiN - Rede de Informação do Departamento de Defesa

ESM - Espaço Cibernético Depende do Espectro Eletromagnético

EUA- Estados Unidos da América

FFAA - Forças Armadas

GAO - *Government Accountability Office*

GPS - Sistema Global de Posicionamento

ISCOM - Centro de Inteligência e Comando

IW – Guerra da Informação

JFHQ-C - Comandante da Sede da Força Conjunta Ciber (JFHQ-C)

MAGTFS - Forças-Tarefas Aéreas Terrestre Marítimas

MARFORCYBER - Comando do Ciberespaço da Marinha e das Forças dos Fuzileiros Navais dos EUA

MCCOG - Grupo de Operações do Ciberespaço do Corpo de Fuzileiros Navais

MCCYWG - Grupo de Guerra do Ciberespaço do Corpo de Fuzileiros Navais

MCEN - Rede Empresarial do Corpo de Fuzileiros Navais

MCEN Ops - Operações de Rede Empresarial do Corpo de Fuzileiros Navais

NCW - *Net Centric Warfare*

NETCOM - Comando de Tecnologia Empresarial da Rede do Exército dos Estados Unidos

NETWARCOM - Comando Naval de Guerra e Redes

NMS-CO - Estratégia Militar Nacional Para Operações Cibernéticas

NSA - Agência de Segurança Nacional

OCO - Operações Defensivas do Ciberespaço

OTAN - Organização do Tratado do Atlântico Norte

OTSC - Organização de Tratado de Segurança Coletiva

RAND - Corporação de Pesquisa e Desenvolvimento

RMA- Revolução de Assuntos Militares

RPC - República Popular da China

RPDC - República Popular Democrática da Coreia

SIGINT - Inteligência de Sinais

TCP/IP – Protocolo de Controle de Transmissão/Protocolo de Internet

TI - Tecnologia de Informação

TIC – Tecnologia(s) de informação e comunicação

TNOSC - Centro de Operações de Segurança de Redes de Teatro

URSS - União das Repúblicas Socialistas Soviéticas

USCYBERCOM – Comando Cibernético dos Estados Unidos

USSTRATCOM - Comando Estratégico dos Estados Unidos

LISTA DE ILUSTRAÇÕES

INTRODUÇÃO

O presente trabalho analisa a inserção do ciberespaço em políticas de segurança dos Estados e suas possíveis implicações para o setor da defesa, ao considerar o ciberespaço como domínio operacional. Para tanto, considera o ciberespaço como domínio operacional, partindo especialmente da perspectiva dos Estados Unidos da América (EUA). A fim de que se possa compreender as origens dessa inserção, faz-se necessário expor um panorama evolutivo que analisa o uso da informação como ferramenta para operações militares. Diante disso, responder a indagação "o que leva os Estados Unidos em considerar o ciberespaço como ambiente para operações militares?" é de extrema importância, pois permite avaliar os efeitos causados pela revolução da informação e como esta impactou nos assuntos militares. Esses impactos provêm fundamentalmente do desenvolvimento de capacidades militares-tecnológicas dos EUA durante a Guerra do Golfo, as quais influenciaram os Estados em aspectos de desenvolvimento militar após o conflito. Diante desse plano contextual, alguns países consideraram o ciberespaço como domínio operacional, resultando em mudanças de entendimento acerca de assuntos estratégicos e em suas doutrinas. Como exemplo dessa mudança em assuntos militares-tecnológicos, será apresentado o Comando Cibernético dos Estados Unidos (USCBERYCOM), que representa uma ferramenta estatal na defesa da liberdade de atuação dos interesses estadunidenses e de seus aliados no ciberespaço.

Cabe destacar que a natureza desse trabalho é de caráter descritivo, documental e bibliográfico, dada a preocupação de identificar os fatores que contribuem para a emergência do tema nos Estudos Estratégicos. É feita uma densa investigação sobre o uso da informação e a respeito das mudanças dos assuntos militares, assim como de artigos especializados, documentos e notícias oficiais do Departamento de Defesa (DoD) que explicam porque os Estados Unidos consideram o ciberespaço um domínio operacional. Uma das principais relevâncias desse trabalho provém da escassez de bibliografia em língua portuguesa sobre o assunto, visto que as maiorias das fontes utilizadas é em língua inglesa.

A divisão do trabalho é feita em três seções. A primeira aborda conceitos relacionados à informação e à sua utilização estratégica e trata, ainda, do desenvolvimento de tecnologias que possibilitam mudanças de cunho militar-estratégico por parte dos Estados. Também são apresentados desdobramentos conceituais no que

tange à guerra cibernética. A segunda seção explica como a guerra cibernética é tratada pelas Forças Armadas (FFAA) dos EUA. Nessa seção, ainda será explanado o USCYBERCOM, expondo como ocorreu sua implementação inicialmente como comando subordinado ao Comando Estratégico (USSTRATCOM). Ademais, explora quais suas atividades operacionais no enfretamento de ameaças cibernéticas e na proteção das redes de defesa. É ressaltada a importância da Força de Missão Cibernética do USCYBERCOM, que se alinha com a estratégia do Departamento de Defesa. Na terceira seção, expõe-se como o espaço cibernético é tratado como domínio de operações, além de apresentar perspectivas de países adversários aos EUA no contexto internacional, como China, Rússia e Coreia do Norte. Por exemplo, a China tem impulsionado cada vez mais o desenvolvimento de suas capacidades cibernéticas, objetivando ampliar seu poderio nacional. A Rússia é tida como uma das maiores ameaças no domínio cibernético em relação aos EUA, por apresentar capacidades equiparadas às da potência norte-americana. Já a Coreia do Norte, que possui um espaço cibernético controlado pelo regime e tem cada vez mais se dedicado a assuntos cibernéticos, inserindo assim em sua estratégia nacional no uso da força contra seus adversários. Os desafios e perspectivas futuras do USCYBERCOM também são abordados nessa seção.

1 CIBERESPAÇO COMO DOMÍNIO MILITAR: CONTEXTO E DEFINIÇÕES

1.1 O Ciberespaço no Contexto da Revolução da Informação e Revolução dos Assuntos Militares

Com a emergência do ciberespaço em políticas de segurança dos Estados, demonstra-se a importância de considerá-lo como domínio de operação. Para melhor entendê-lo, faz-se necessária a elucidação de assuntos relacionados à Revolução da Informação, pois ela possibilitou mudanças militar-tecnológicas na forma com que os Estados conduzem seus assuntos militares.

Nesse intento, a rapidez da propagação da informação no século XXI vem atingindo, cada vez mais, um grande número de pessoas. Isso acontece por conta dos frequentes avanços tecnológicos que possibilitam uma circulação mais rápida dos dados. Por conta disso, a informação irá melhorar a habilidade de destruição, como também poderá contribuir para o desenvolvimento de capacidades disruptivas. Como apontado por Arquilla e Ronfeldt (1997), na Era da Informação, forças concentradas serão utilizadas em ataques menores e de natureza mais inteligente. Além disso, os autores afirmam que:

> "duelos decisivos pelo controle de informação irão substituir os campos de batalhas de atrito ou aniquilação; a exigência de destruir irá diminuir e a capacidade de interromper será aprimorada" (ARQUILLA; RONDFEDT, 1997, p. 2).

Dessa forma, o aprimoramento de armas militares-tecnológicas pode mudar padrões em conflitos armados devido à maior precisão de seus ataques.

Vale salientar que o atual contexto global é marcado pelos frutos da revolução da informação, isto é, a sociedade vigente usufrui de notáveis tecnologias que proporcionam rápidas trocas de informação, as quais, por sua vez, dão suporte a inovações relacionadas à gestão e à teoria organizacional. Assim, uma vez que as instituições modernas, em especial as militares, são organizadas de forma hierárquica, a revolução da informação está não só desafiando suas configurações (DAVIS, 1997), mas também apresentando novos horizontes para o poder militar.

Dessa forma, a força e a rapidez com que a informação é propagada resulta em revoluções tecnológicas, em que é possível ser criado um novo ambiente para as

relações humanas chamado espaço cibernético. Para melhor compreender o que é e como ele funciona, faz-se necessária uma elucidação no que se refere ao fenômeno chamado de revolução da informação (CALVETY, 2008).

Tomando por base as ideias de Zacher e Castells, Calvety (2008) afirma que a revolução da informação foi um dos propulsores de mudanças fundamentais nas relações internacionais, em que a disseminação de ideias e transferência de dados estão cada vez mais intrínsecas em nosso cotidiano como também em segmentos inteiros da vida pública, como setores de cultura, negócios e entretenimento, que têm sido revolucionados por novas tecnologias (CALVETY, 2008). Nesse contexto, a revolução da informação[1] ocorre devido aos "avanços tecnológicos realizados e que aumentaram a capacidade de coletar dados precisos" (DAVIS, 1996, p. 83) em que podem suceder mudanças nos meios para a guerra, como também os objetivos que podem ser alcançados. Além do mais, em uma guerra futura, de acordo com Davis (1996), haverá uma competição pela luta da informação, visto que a informação pode ser um instrumento que possibilitará o desenvolvimento de sistemas de comando e controle militares projetados para coordenar o emprego de equipamentos que podem ser decisivos no tempo e no espaço. Nessa esteira, conclui-se que a revolução da informação foi fundamental para o desenvolvimento do espaço cibernético. Como descreve Nye Jr (2011), os líderes políticos estão assimilando a capacidade transformadora destas tecnologias, visto que os estudos acerca da segurança cibernética têm ganhado destaque não só entre especialistas em informática.

Outrossim, Arquilla e Rondelft (1993), em sua obra "*Cyberwar is Coming!*", explanam que a revolução da informação pode ser entendida como:

> um reflexo do avanço da informação informatizada e tecnologias de comunicação em que informações são coletadas, armazenadas, processadas, comunicadas e apresentadas com o intuito de buscar uma maior vantagem no aumento de informações. (ARQUILLA; RONDELFT, 1993, p. 143, tradução nossa).

Sendo assim, a revolução da informação pode ser utilizada como recurso estratégico na era industrial[2]. Desse modo, é possível afirmar que as variadas organizações, sociedades e atores internacionais têm se beneficiado da revolução da

[1] Exemplos de tecnologia desse campo: computadores, modem, cabos de rede, LED e LCD.
[2] A literatura mais contemporânea que versa sobre a revolução da informação considera que atualmente a era em vigor é um período pós-Era Industrial, a chamada Era da Informação.

informação, pois esta possibilita um melhor ganho de tempo e aperfeiçoamento de tarefas.

Cabe destacar que a relevância da informação não é apenas uma característica dos dias atuais; ela sempre esteve presente durante a história da humanidade (CALVETY, 2008). De acordo com Calvety (2008), os avanços científicos desempenharam papel importante em mudanças no processo de comunicação e transmissão de informações. Dessa maneira, possibilitou moldar a história, as atividades humanas e também as instituições. Salientando, ainda, os processos que abordam a informação, é notório que o determinismo tecnológico entende o mundo moderno como propenso a passar por novas fases históricas; sendo assim, resultaria em um processo de desenvolvimento tecnológico constante (CALVETY, 2008).

Além disso, Calvety (2008) aponta que a fusão dos computadores com as telecomunicações fez com que o sistema de comunicações multimídia alcançasse novos níveis de expensão a baixos custos, ou seja, proporcionasse uma transformação relevante em aspectos de como se configuram os processos de comunicação e interação. É notório que um dos impactos dessa revolução culmina em uma expansão de aspectos relacionados ao desenvolvimento de tecnologias e também a uma maior disponibilidade de ferramentas. A forma com que essas novas tecnologias de informação se disseminam é realizada de forma desigual pelas organizações, sociedades e atores internacionais (CALVETY, 2008).

Nesse interim, a revolução da informação possibilitou aos Estados desempenharem melhorias nas suas capacidades militares-tecnológicas. Embora, de acordo com Gardner (2005), a revolução tenha desempenhado melhorias no setor militar, ela não alterou totalmente a lógica geoestratégica e o contexto político-econômico (GARDNER, 2005). Aparatos como computadores, satélites e mecanismos provedores de rápido acesso a informações foram importantes para que uma revolução nos assuntos militares[3] fosse possível, como pode ser comprovado em eventos como as Guerras do Golfo, de 1990 a 1991, e do Iraque em 2003 (GARDNER, 2005).

Nessa esteira, cabe destacar que as inovações nos computadores e comunicações foram fundamentais para aumentar as precisão e velocidade das capacidades militares nos dias atuais, como também desencadearam maior proliferação do crime e de atividades terroristas. Dessa forma, existe uma preocupação de que as novas tecnologias

[3] Fenômeno citado será explicado mais adiante no texto, página 18.

de informação e comunicação (TIC) sejam "sementes de sua própria destruição". Em outras palavras, devido à vinculação de suas atividades como *networking*[4], as TIC podem também representar riscos, uma vez que, mediante sabotagem cibernética, os sistemas de tecnologia de informação podem ser interrompidos ou, até, destruídos por Estados ou grupos antiestatais, através, por exemplo, da implementação indevida de cavalos de Troia, *hacking*, ataque de negação de serviço (DoS), dentre outros (GARDNER, 2005).

Percebe-se, então, que há uma proliferação da tecnologia de comunicação, a qual Calvety (2008) observa que:

> ocorre de forma desigual, mas em constância entre organizações, sociedades e entre atores internacionais. Retornar para os modos anteriores é quase impossível: sociedades em países desenvolvidos já dependem fortemente das tecnologias, não só para o armazenamento de informações, mas também para seu processamento, com o objetivo de permitir que essas tecnologias executem tarefas cada vez mais exigentes (CALVETY, 2008, p. 19, tradução nossa).

As novas TIC também mudaram o comportamento dos governos: de acordo com Ethredge (1985 apud NYE JR, 2012), com estudo e experiência, os novos conhecimentos gradualmente são levados em consideração pelos interesses nacionais, resultando, assim, em novas políticas. No período de pós-11 de setembro, ao *World Trade Center* e Pentágono, Gardner (2005) explana que esse acontecimento despertou maior interesse de desenvolvimento e inovação na área de segurança cibernética, em que investimentos prioritários fossem direcionados para tecnologias mais sofisticadas, com o intuito de proteger os serviços de informação (GARDNER, 2005).

No que concerne ao caso dos Estados Unidos, a *Defense Advanced Research Projects Agency* (DARPA), que detém atividades ligadas ao Departamento de Defesa daquele país, foi responsável por criar uma diversidade de tecnologias, com o objetivo de lutar na "guerra global contra o terror". Baseado no plano estratégico lançado em 2007, sobre o papel da DARPA pode-se afirmar que "fornece tecnologias para todo o Departamento [de Defesa] e é projetada para ser um 'motor tecnológico' especializado para transformar o Departamento de Defesa" (DARPA, 2007, p. 6, tradução nossa). Além disso, o documento ressalta que a abordagem da DARPA é "imaginar as capacidades de que um comandante militar pode precisar e acelerar essas capacidades através de demonstrações de tecnologia". Ademais, a DARPA funcionaria "como uma

[4] Processo em que dois ou mais computadores possam compartilhar informações.

costura entre os serviços militares para desenvolver novas e verdadeiras capacidades conjuntas que nenhum serviço militar poderia ser realizado por si só" (DARPA, 2007, p. 6, tradução nossa).

A Internet foi uma das tecnologias desenvolvidas pela DARPA, em meados das décadas de 1960 e 1970, com o desenvolvimento do Protocolo de Controle de Transmissão/Protocolo de Internet (TCP/IP). Vale ressaltar que as mudanças proporcionadas pela DARPA foram fundamentais para as redes computacionais públicas e privadas que abrangem o DoD, o governo federal e a indústria nos EUA e no mundo (DARPA, 2007).

Dentro desse contexto, a Revolução dos Assuntos Militares (RMA) emergiu entre os especialistas em segurança como uma representação de ideias e abordagens em assuntos relacionados a políticas de segurança (CHAPMAN, 2003). Nessa conjuntura, Champan (2003) elucida que os primórdios do pensamento atual a respeito da RMA derivam da abordagem realizada pela Rússia no início dos anos 1980, quando o marechal soviético Nikoklai Ogarkov apontou que uma "revolução técnica militar" seria capaz de melhorar a capacidade de letalidade, como também a eficácia de armas convencionais. Como Secretário-chefe do gabinete soviético da época, Ogarkov e sua equipe sabiam do interesse dos Estados Unidos em investir no desenvolvimento de tecnologia computacional. Desse modo, trouxe preocupação às Forças Armadas soviéticas, pois estavam conscientes das incapacidades perante o inimigo norte-americano no embate relacionado à tecnologia de computadores.

Nessa esteira, as ideias soviéticas migraram para o Departamento de Defesa dos Estados Unidos, até então chefiado por Andrew W. Marshall, que defendia uma revolução militar. Marshall criticava as preferências por serviços militares tradicionais, influenciando assim um grande número de intelectuais especializados em políticas de segurança nos EUA (CHAMPMAN, 2003).

No que tange à RMA, é imprescindível expor a importância da Guerra do Golfo, de 1990 a 1991, devido à utilização estadunidense de uma grande quantidade de sistemas de armas que possuíam tecnologia de ponta (DAVIS, 1996). Nesse segmento, pensadores militares americanos, como David Rondfeldt e John Arquilla, ressaltaram a vitória dos Estados Unidos e aliados contra o Iraque neste conflito, podendo ser observada a preservação de suas redes e o rompimento das adversárias. Assim, os autores elucidaram sobre o paradigma da guerra em rede, afirmando que armamentos de grande porte operando em comandos centralizados poderia não ser a melhor opção para

esse conflito. Em vez disso, pequenas unidades operantes dentro de redes representavam agentes mais efetivos, e a Internet seria um importante componente em campo de batalha. A partir disso, foi de conhecimento que fatores como velocidade, conhecimento e precisão diminuiriam casualidades e resultariam numa maior rapidez, como pode ser observado na Guerra do Golfo, e também uma progressiva mudança do campo de batalha físico para o domínio virtual (CALVETY, 2008).

Todavia, com os desdobramentos posteriores, a Guerra do Golfo foi notada como uma ampliação do duplo debate desencadeado pelos benefícios proporcionados pelo 'diferencial de informação' C4I[5], bem como experiências com a ameaça de invasão de *hackers* durante o conflito. Também havia preocupação em torno de uma possível invasão de *hackers*, pois na época do conflito, os Estados Unidos utilizaram a Internet para transmitir as ações, em algumas vezes até sem criptografia, representando assim um perigo aos seus serviços de informação (CALVETY, 2008).

Nessa conjuntura, outros países são desafiados a buscar novas alternativas para modernizar suas capacidades militares. Desta forma, o conceito de RMA pode ser variável, devido às mais diversas interpretações, como exemplificado pela China, que exaltou a relevância da RMA, afirmando que abandonaria o comprometimento com o exército armado e apostaria mais em assuntos relacionados à modernização militar (CHAMPMAN, 2003).

Como posto por Champman (2003), existiu, nas décadas de 1990 e 2000, um debate caloroso a respeito da RMA. Críticos como Stephen Biddle, Max Boot e Collins Gray questionam a utilização do termo "revolução", para apontar em que a tecnologia militar impactou na mudança na guerra e nas Forças Armadas (FFAA). Outros pensadores afirmam que pode ser perigosa a forma pela qual o assunto tem sido conduzido, pois acarreta um excesso de confiança na capacidade de a tecnologia vencer guerras e, assim, uma maior probabilidade de gerar conflitos. Já outros críticos afirmam que existe de fato uma revolução nos assuntos militares, mas que ela não é tecnológica, e sim pelo confronto de atores não-estatais, ou seja, de redes globais de terroristas. Outro ponto de vista apresentado por alguns críticos é o de que a RMA seria uma motivação para que a corrida armamentista continuasse após anos de Guerra Fria (CHAMPMAN, 2003).

[5] Comando, Controle, Comunicações, Computadores e Inteligência.

Ainda sobre a RMA, é evidente que, durante da década de 1990, Andrew W. Marshall e sua equipe a definiram como:

> uma grande mudança na natureza da guerra provocada pela aplicação inovadora das tecnologias que, combinadas com mudanças dramáticas na doutrina militar e nos conceitos organizacionais, alternaram fundamentalmente o caráter e a conduta de operações militares (SLOAN, 2012, p. 3, tradução nossa).

Sendo assim, as tecnologias militares são fatores primordiais para a RMA. Foram utilizadas durante a Guerra do Golfo e também em conflitos posteriores, como a Guerra do Afeganistão, de 2001 a 2002, e do Iraque. Os avanços podem ser exemplificados pelo uso de munições guiadas com precisão (PGMs), Inteligência, coleta, vigilância e reconhecimento (ISR) e C4I (SLOAN, 2012).

Por conseguinte, conflitos como o do Iraque revelaram que a tecnologia ainda não se demonstrou totalmente capaz de substituir o uso de soldados contra adversários, haja vista que, por exemplo, o uso do poderio aéreo não se demonstrou suficiente para a ruína do regime de Hussein. Desta maneira, é desafiador afirmar que uma revolução possa ter ocorrido pelo simples fato do impulsionamento da elaboração e modernização de equipamentos militares em um determinado período de tempo (CHAMPMAN, 2003). Consequentemente, as revoluções não são entendidas apenas por um maior desenvolvimento de tecnologia, mas são profundas mudanças no *status quo* existente, isto é, expressadas pelo processo ativo de requerer uma adaptação efetiva por parte de indivíduos e organizações, para que ocorra de forma bem-sucedida (DAVIS, 1997). Dessa forma, para elucidar sobre componentes de uma RMA, Krepinevitch (1994) aponta que a tecnologia, o desenvolvimento de sistemas, a inovação operacional e a adaptação organizacional:

> são, por si só, necessários, mas não suficientes, para a realização dos grandes ganhos nas forças armadas. A eficácia é o que caracterizaria as revoluções militares. Em particular, enquanto os avanços na tecnologia geralmente realizam revolução militar, eles sozinhos não constituem a revolução. O fenômeno é muito mais abrangente e consequência da inovação tecnológica, por mais dramática que seja (KREPINEVITCH, 1994, tradução nossa).

Nessa esteira, as revoluções militares ocorrem quando são realizadas novas aplicações de tecnologias em que são exercidas em um número expressivo de sistemas militares que pode ser entendido como operações inovadoras, mudando assim a

condução do conflito, podendo ocasionar uma magnitude da eficácia em que as forças armadas podem se organizar (KREPINEVITCH, 1994).

Desse modo, a Revolução da Informação possibilitou mudanças no entendimento dos Estados em RMA, podendo adequar suas novas perspectivas, devido às ameaças cibernéticas, mudando assim o posicionamento da política dos Estados e seus desdobramentos para defesa e segurança, principalmente no que se refere à guerra cibernética.

1.2 Guerra cibernética

A emergência do espaço cibernético como novo domínio de combate e o estabelecimento do USCYBERCOM pelo Departamento de Defesa expressam a preocupação dos Estados Unidos na manutenção de seus interesses nessa área emergente (FOLKS, 2011).

Nos anos 1990, com a explosão das capacidades das tecnologias de informação, o conceito de *Net-Centric Warfare* (NCW) emergiu e colocou as redes de informação em papel de destaque nas guerras. Aplicações de NCW deram suporte às Forças Armadas dos Estados Unidos no espectro de capacidades, podendo ser exemplificado pelo desenvolvimento do Sistema Global de Posicionamento (GPS), sendo indispensável por fornecer a localização em campo de batalha (WOGAMAN, 1998).

A Era da Informação e a disseminação das TIC trazem consigo desafios na elaboração de políticas nacionais e internacionais entre acadêmicos e políticos nos debates acerca da abrangência das explicações da guerra cibernética, que decorre da Revolução da Informação e da RMA (CEPIK; CANABARRO; BORNE; 2015). Foi dentro desse contexto que o termo guerra cibernética ganhou repercussão nos anos 1990, especialmente com a publicação do artigo de John Arquilla e David Rondfeld intitulado "*Cyberwar is Coming*!", publicado pela RAND Corporation em 1993. Cabe destacar que esta Corporação desenvolve soluções de políticas públicas em diversas áreas e também setores militares. Desse modo, Arquilla e Rondfeld (1993) reconheceram certo nível de potencialidade de ataques digitais durante a Guerra do Golfo.

Ainda para Arquilla e Rondfeld (1993), com a revolução da informação, este

processo representa mudanças de como as sociedades podem realizar conflitos. Para melhor compreensão, é necessário ser realizada uma diferenciação básica entre *netwar* e guerra cibernética. No que toca a *netwar*, é entendido que:

> refere-se a um grande nível de conflitos relacionados à informação entre nações ou sociedades. Significa tentar interromper, ou danificar, ou modificar o que uma população-alvo conhece ou pensa de si mesma, bem como do mundo que a rodeia. Uma rede pode se concentrar em opinião pública ou de elite, ou ambos. Pode envolver a diplomacia pública como medidas, propagandas, campanhas psicológicas, políticas, subversão cultural, interferência com a mídia local, infiltração de redes e bancos de dados informáticos, isto é, *netwar* apresenta uma nova entrada no espectro de conflito que abrange setores econômicos, políticos, sociais e militares (ARQUILLA; RONDFELDT, 1993, p. 145, tradução nossa).

Assim, com a *netwar*, podem surgir outros tipos de redes entre governos e atores não-estatais, provocando disputas de governos contras grupos lícitos e organizações terroristas, também na proliferação de armas de destruição em massa ou contrabando de drogas. Outra forma em que esse fenômeno ocorre é quando atores não-estatais rivais entram em conflito e os governos têm a preocupação de observar o embate para que não causem danos colaterais aos interesses nacionais, ou chegando até a apoiar um dos lados, sendo, assim, a forma mais especulativa de *netwar* (AQUILLA; RONDFELDT, 1993).

Já sobre a guerra cibernética, Arquilla e Rondfeldt (1993) elucidam que ela:

> Refere-se à conduta e à preparação de operações militares, de acordo com os princípios relacionados à informação. Isso significa interromper, se não destruir, informações e sistemas de comunicação, amplamente definidos para incluir até na cultura militar, pois um adversário procura conhecer: quem é, onde está, o que pode fazer, quando, por que está lutando, quais ameaças contornar primeiro e assim por diante (ARQUILLA; RONDFELDT, 1993, p. 146, tradução nossa).

A forma dessa guerra pode envolver diversos tipos de tecnologias, entre elas a C^3I^6; para coleta, processamento e distribuição de informações; para comunicações táticas, posicionamentos e identificação de amigo-ou-inimigo; e para sistemas de armas "inteligentes". Baseado na literatura sobre a revolução da informação, pode-se observar que o fenômeno demanda inovações organizacionais para diferentes partes de uma instituição, ou seja, a guerra cibernética pode implicar alguma reorganização institucional (ARQUILLA; RONDFELDT, 1993).

Sobre os desdobramentos da guerra cibernética, é possível salientar que essa tipo

[6] Comando, Controle, Comunicação e Inteligência.

de guerra gera uma forma de "cegueira" eletrônica, causando uma série de falhas ao adversário – como bloqueio, sobrecarga e invasão de informações –, podendo ter amplas implicações para organizações e doutrina militar, de modo que a revolução da informação exija inovações organizacionais, as quais são necessárias para uma maior conexão de redes, ao contrário de uma série de hierarquias separadas. Além do mais, a guerra cibernética pode resultar em discussões acerca de organização e doutrina militar, como também melhorias de estratégias, táticas e *design* de armas (ARQUILLA; RONDFELDT, 1993).

Ainda sobre a guerra cibernética, a obra "*Cyberwar: The Next Threat to National Security and What to do About It*", de Richard A. Clarke e Robert K. Knake, é de bastante relevância para os estudos relacionados ao assunto. A seguir, eis o que os autores dissertam sobre guerra cibernética:

> É a penetração não autorizada, em nome ou em apoio de um governo de outra nação a computador ou rede, ou qualquer outra atividade que afeta um sistema de computador, no qual o objetivo é adicionar, alterar ou falsificar dados ou causar o rompimento ou danos a um computador, ou dispositivo de rede, ou os objetos de controles do sistema de computador (CLARKE; KNAKE, 2015, p. 150).

Nesse interim, o termo guerra cibernética ainda é entendido como "ações de Estado-nação para invadir computadores ou redes de uma nação com intenção de causar danos e transtornos" (CLARKE; KNAKE, 2015, p. 11).

Outros autores ainda destrincham sobe a guerra cibernética. Por exemplo, Nye Jr (2012) a define como "ações hostis no ciberespaço que têm efeitos que amplificam ou são equivalentes a grandes violências cinéticas" (NYE JR, 2012, p. 21). Desse modo, é pertinente que sejam apontadas características que diferem sobre o que acontece no mundo físico e no mundo virtual. No mundo físico, os governos possuem quase o monopólio em larga escala do uso da força, o defensor possui um conhecimento do terreno e os ataques só acabam por causa do atrito e da exaustão. Em contraposição, no mundo virtual os atores podem ser diversos e até ter suas identidades postas em anonimato, a distância é imaterial e os custos de uma ofensiva muita das vezes podem ser considerados baixos (NYE JR, 2012). A guerra cibernética é tida como a mais dramática das ameaças cibernéticas, visto que os principais Estados, com o suporte de elaborados recursos técnicos e humanos, poderiam causar uma ruptura abrupta e acentuada via ataques cibernéticos em alvos militares ou civis. É importante destacar que a guerra cibernética e a espionagem econômica estão ligadas amplamente com os

Estados. O crime cibernético e o terrorismo cibernético estão geralmente associados a atores não-estatais (NYE JR, 2012).

Pode ser observado que os assuntos relacionados à guerra cibernética ainda estão em processo de maturação, porque, segundo alguns especialistas, apenas em 2007, na Estônia, foi protagonizado o que é descrito como a primeira guerra no ciberespaço, uma ofensiva que se estendeu por um mês e obrigou as autoridades estonianas a defender seu país de uma série de ataques digitais que, para alguns, foi acionada por ordens originadas da Rússia ou de fontes russas, em retaliação à retirada de uma estátua de bronze de um soldado da 2ª Guerra Mundial num parque da cidade portuária báltica de Tallinn (DAVIS, 2007). Os ataques ao ciberespaço da Estônia resultaram numa degradação ou perda de serviço temporária de servidores comerciais e governamentais. A grande variedade de ataques Negação de Serviço Distribuído (DDoS), foi direcionada a *sites* públicos e *e-mail*s, outros foram concentrados em alvos vitais, tais como serviços bancários *online* e DNS (OTTIS, 2008).

Neste momento, dando enfoque na maneira com que os Estados Unidos abordam a temática, os maiores custos são configurados em termos de espionagem e crime, mas que, na próxima década, guerra e terrorismo podem exigir mais esforços do que exercem hoje em dia (NYE JR, 2012). Dessa maneira, como evidencia o discurso do então Secretário de Defesa estadunidense William J. Lynn III, no Workshop Anual Internacional de Segurança de 2011, em Paris, é necessário que exista um debate sobre os desafios de segurança que permanecem durante o presente e de possíveis mudanças que vão moldar o futuro do ambiente estratégico, sendo um deles a ameaça de ataque em redes de computadores. Além disso, cada vez mais com a escalada da ameaça cibernética, certos grupos que detêm recursos nessa área podem expandir suas atividades em direções incertas o que pode representar um perigo para agências de Inteligência estrangeiras e para as dos Estados Unidos também.

1.3 Ciberespaço como domínio

A princípio, é necessária uma contextualização do ciberespaço e sua inserção nos Estudos Estratégicos, pois o ciberespaço ainda apresenta características que estão em debates recorrentes por estadistas e acadêmicos, de modo que há uma relação deste espaço com assuntos ligados à segurança internacional e à defesa nacional (BOHN;

NOTHEN, 2016).

Na década de 1940, pode ser observada a definição de um subcampo organizado de conhecimento de Estudos Estratégicos, pois era relevante o estudo mais detalhado entre a política, a guerra e o uso das forças pelos Estados com as duas Grandes Guerras. Mesmo com a definição de Estudos Estratégicos ser ligada à utilização de força por entidades estatais, este campo possui uma diversidade de estudos e possui um caráter interdisciplinar, existindo uma preocupação nos mais variados desdobramentos em relação aos diferentes domínios (BOHN; NOTHEN, 2016).

Durante a década de 1990, inúmeros autores destrincharam sobre o que poderia ser entendido por Guerra da Informação (IW), que, por definição, representaria um campo de crescente evolução em que desperta o interesse de planejadores relacionados a assuntos de defesa e formuladores de políticas. Devido a essas mudanças, os EUA e aliados procuraram explorar melhor essas infraestruturas de informação global em evolução, visando tecnologias com intuito militar (MOLANDER; RIDDILE; WILSON, 1996).

Devido a diversas incertezas que o assunto apresentava, em 1995, o Secretário de Defesa dos EUA formou um Conselho Executivo da IW que pretendeu facilitar o desenvolvimento em assuntos nacionais relacionados à Guerra de Informação. Nesse mesmo pedido, foi solicitado também que a RAND fornecesse estrutura analítica para identificar as principais questões da IW, como também procurar desenvolver um entendimento geral sobre o assunto nos EUA, e assim visar a uma estratégia. Além disso, houve preocupação em produzir uma estrutura necessária para o aprimoramento de políticas, estratégicas e metas estratégicas da IW (MOLANDER; RIDDILE; WILSON, 1996).

Assim, com o crescente destaque do espaço cibernético em assuntos de cunho estratégico, cada vez mais os Estados têm se empenhado na regulação do ciberespaço como um novo domínio estratégico. Dessa maneira, políticas e estratégias nacionais de países como Estados Unidos, França, Reino Unido e Alemanha servem como exemplos do uso de políticas referentes à defesa cibernética, já que com a era da informação, as redes e os dados cada vez mais ganharão espaço de destaque nas estratégias político-militares dos Estados (BOHN; NOTHEN; 2016).

Bohn e Nothen (2016) afirmam que o espaço cibernético é extremamente mutável, e dessa forma os países comportam-se de maneira em que instituições e protocolos possam ser adaptados e assimilados de forma rápida, potencializando o uso

desse espaço, da maneira mais estrategicamente eficaz possível. Em congruência no que se refere ao ciberespaço, Kuehl (2009) afirma que "o espaço cibernético é um domínio operacional[7] caracterizado pelo uso de eletrônicos e do espectro eletromagnético parar criar, trocar, modificar e explorar informações sistemas fundamentados em tecnologia de informação".

No que tange ao espaço cibernético, Sheldon (2011) o caracteriza como "um domínio em que as operações cibernéticas ocorrem" (SHELDON, 2011, p. 96). Ainda, Sheldon (2011) destrincha as características do espaço cibernético, o qual depende do espectro eletromagnético (ESM), isto é, o espaço cibernético não pode existir, caso não esteja apto para conduzir energia eletromagnética. Sem o ESM, milhões de informações e Comunicações e Tecnologias (ICT) não poderiam se comunicar uns com os outros. Outra característica do espaço cibernético é apresentar-se como único domínio em que precisam de objetos feitos pelos homens para existir. Placas de circuitos integrados, semicondutores, microchips, condutores e outras ICTs são essenciais para o estabelecimento do ESM. Outra característica do espaço cibernético é que ele pode ser replicado, diferentemente do que acontece em outros domínios, já que existe apenas um ar, um mar, um espaço e uma terra. É exposto que os custos de entrada no espaço cibernético podem ser relativamente baixos, ou seja, exige uma quantia moderada de investimentos se comparado com a de outros domínios (SHELDON, 2011).

Com o aumento dos ataques cibernéticos, o tema sobre defesa no ciberespaço é tido como de grande importância militar para os Estados Unidos. Bohn e Nothen (2016) apontam que a chamada RMA intensifica relevância da questão cibernética, ou seja, refere-se à "[...]interação entre sistemas que coletam, processam, integram e comunicam informação, e aqueles que aplicam a força militar, com o objetivo de criar a violência de precisão" (BOHN; NOTHEN, 2016, p. 98-99). Por conseguinte, ainda em concordância com os autores, os EUA consideram o ciberespaço como um domínio próprio para a guerra.

Lynn III (2010) evidencia o discurso de que o ciberespaço deve ser reconhecido como um domínio igual à guerra por terra, mar, ar e espaço. Com o intuito de facilitar as operações no ciberespaço, o Departamento de Defesa precisaria de uma estrutura organizacional adequada. Em relação à postura defensiva, seria importante que os EUA fossem dinâmicos e rápidos na resposta a ataques cibernéticos. Para isso, o Pentágono,

[7] Capacidade de desenvolver meios militares de realizar guerra em determinado espaço.

por meio do seu Comando Cibernético (USCYBERCOM) implantou um sistema que mantém *software* de segurança e *firewalls* atualizados e uma linha de proteção de Inteligência que o governo fornece às defesas especializadas (LYNN III, 2010).

Ainda no que tange aos aspectos da defesa cibernética, é entendido que deve haver cooperação com os seus países aliados no objetivo de monitorar redes informáticas de futuras invasões, assim como já ocorre em defesas aéreas e espaciais. Acordos mais concretos são considerados essenciais no compartilhamento de informação, tecnologia e Inteligência, sempre visando um número maior de aliados (LYNN III, 2010).

Krepinevitch (2012) trata o ciberespaço como domínio de operações, pois há mudança no caráter da guerra com a competição militar que se expande no domínio cibernético. Ainda afirma que o domínio cibernético tem sido uma área de competição entre Estados e atores não-estatais em que líderes políticos e militares relatam que as capacidades das armas cibernéticas são surpreendentes (KREPINEVITCH, 2012).

Como visto, devido à competição dentro do espaço cibernético, ocorre a emergência de ameaças, uma vez que vários Estados detêm, em maior ou menor grau, capacidades cibernéticas. Assim, os Estados tendem a buscar melhorias que os coloquem à frente dos seus adversários, como exemplificado Jaffer e Brunet (2017), que narram o testemunho do ex-Diretor de Segurança Nacional e ex-Comandante do USCYBERCOM General Keith B. Alexander, que, por sua vez, afirma que, mesmo com os benefícios que a tecnologia pode trazer para a sociedade, ela também é vista como uma maneira pela qual atores "ruins" podem atacar os EUA. Além disso, afirma que desenvolver mais estratégias e doutrinas é importante e que a nação norte-americana deve entender que são necessárias melhores ações que possam deter a atuação de adversários no domínio cibernético (JAFFER; BRUNET, 2017).

No que tange aos atos de guerra no ciberespaço[8], Jaffer e Brunet (2017) apontam, de forma hipotética, que suas consequências poderiam consistir em grandes perdas de vidas, destruição ou incapacidade de infraestruturas essenciais ou até mesmo ataques que poderiam causar grandes danos econômicos. É importante elucidar que até o momento os danos cinéticos de ataques cibernéticos são restritos, com exceção do

[8] Na obra de Libicki (2012), "Cyberspace is not a Warfighting Domain", é discutido porque o domínio cibernético não é considerado um domínio de guerra.

caso envolvendo o Stuxnet[9]. Conforme o testemunho do General Keith B. Alexander, sobre as atividades dos EUA no ciberespaço, é entendido que:

> Mesmo que essas atividades subam para o nível de ato de guerra ou não – vale a pena considerar como os EUA podem se defender melhor contra essas atividades. Hoje, os inimigos dos Estados Unidos não precisam atacar nosso governo para ter efeito estratégico nacional substantivo. Na verdade, atacar a infraestrutura civil ou econômica pode ser uma abordagem mais eficaz na era moderna. [...]O futuro da guerra está aqui, e precisamos entender como arquitetar os EUA para essa nova realidade. (JAFFER; BRUNET; 2017, p. 33, tradução nossa).

Pode-se dizer que o cenário apontado pelo Comandante seja um estudo de tendência, uma vez que o entendimento da guerra no espaço cibernético ainda é controverso, por isso se faz necessário entender como os EUA compreendem o espaço cibernético como domínio operacional.

Krepinevitch (2012, tradução nossa) também cita o General Keith B. Alexander, sobre o domínio cibernético, em que o general afirma que o "domínio cibernético em alguns aspectos é como o domínio do ar, em ser um reino que não tinha relevância para o planejamento militar, até que, de repente, uma tecnologia ofereceu acesso a ele".

Dessa forma, a percepção dos EUA sobre o ciberespaço é a de que este é um "domínio" em que o combate acontece e no qual os EUA devem dominá-lo (CLARKE; KNAKE, 2010). Em congruência, a Estratégia Militar Nacional para Operações Cibernéticas (NMS-CO), no aspecto de definição do ciberespaço como domínio, entende que este consiste em "um domínio caracterizado pelo uso de eletrônicos e espectro eletromagnético para armazenar, modificar e trocar informações via sistemas de rede e infraestruturas físicas associadas" (FAHRENKRUG, 2007, p. 1).

Para a Estratégia Cibernética do Departamento de Defesa dos Estados Unidos (DoD), de abril de 2015, a respeito do modo de atuação estadunidense para com o ciberespaço, o Departamento de Defesa é responsável por defender os EUA de ataques adversários que possam prejudicar os interesses do país, durante períodos de paz, crise ou conflito. Em maio de 2011, o DoD lançou uma nova estratégia que estabeleceu metas e objetivos estratégicos das missões para os cinco anos posteriores. Desse modo, o documento expõe pontos importantes para que possam ser atingidos os objetivos daquela Pasta de Defesa, entre os quais estão a criação de capacidades de segurança cibernética efetivas e a possibilidade de operações cibernéticas no intuito de defender

[9] *Worm* que infectou centrífugas iranianas relacionadas ao enriquecimento de urânio.

redes. Além disso, é importante ressaltar a capacidade de defender o país contra ataques cibernéticos e também fornecer suporte a planos operacionais (DEPARTMENT OF DEFENSE, 2015).

O Departamento de Defesa norte-americano realiza diversas parcerias com setores privados e parceiros internacionais, com o intuito de melhorar a segurança cibernética coletiva e proteger os interesses dos EUA, alé de melhorar sua estabilidade de estratégia global. A primeira atividade desempenhada pelo DoD é o compartilhamento de informações e cooperação interagências, buscando distribuir informações e coordenar órgãos do governo, para uma atuação integrada, dada a variedade de atividades cibernéticas. Com uma melhor capacidade de organização, é possível que aquele país se defenda contra uma diversidade de ataques cibernéticos e melhor sincronize as operações no ciberespaço. A segunda atividade diz respeito ao enfoque na cooperação com a iniciativa privada, já que empresas desse setor desenvolvem tecnologias que compõem o espaço cibernético, fazendo com que o uso intensivo dessas redes abra janelas que aumentem a vulnerabilidade e oportunizem ataques aos EUA. Além disso, o Departamento de Defesa designa ao setor privado a construção de suas redes, em que são realizados pesquisa e desenvolvimento de capacidades avançadas para o Departamento. A terceira atividade diz respeito à manutenção de alianças, coalizões e parcerias no exterior, isto é, o DoD desempenha um papel como aliado, a fim de entender as ameaças cibernéticas e construir capacidades para defender suas redes e dados. Conjuntamente, os Estados Unidos formam fortes alianças e coalizões para combater os adversários nas mais diversas atividades cibernéticas, firmando atividades com o Oriente Médio, Ásia-Pacífico e Europa (DEPARTMENT OF DEFENSE, 2015).

As missões primárias no ciberespaço estabelecidas pelo Presidente Obama tiveram como objetivo planejar princípios e processos de governança, no intuito de planejar, desenvolver e utilizar recursos dos EUA para garantir, de forma consistente, a atuação do Departamento de Defesa a nível nacional e internacional. A primeira missão do DoD é proteger seus conjuntos de redes, sistemas e informações, pois seus militares dependem muito do espaço cibernético (CLARKE; KNAKE, 2015), o que levou o então Secretário de Defesa a declarar o domínio como operacional, a fim de organizar, treinar e equipar forças militares daquele país. Ainda, o DoD deve estar capacitado para defender suas próprias redes contra ataques e recuperar-se rapidamente caso a missão falhe. Além disso, o DoD procura maior capacitação para operar em um ambiente em

que o espaço cibernético pode ser contestado. Na segunda missão, o Departamento de Defesa deve estar preparado para defender os EUA e seus interesses de ataques que possam produzir consequências negativas as suas redes. Dessa maneira, os ataques cibernéticos são avaliados caso a caso, com base no Presidente dos EUA e em sua equipe de segurança, dentro dessas consequências significativas estão a perda de vidas, danos significativos a propriedades e graves consequências na política externa. As operações cibernéticas podem ser guiadas pelo Presidente ou pelo Secretário de Defesa para evitar um ataque à pátria estadunidense. A terceira missão consiste no dever do DoD de fornecer capacidades cibernéticas integradas para apoiar operações militares e planos de contingência, se dirigidos pelo Presidente ou pelo Secretário de Defesa, os quais são responsáveis por conduzir as operações e assim tentar desestabilizar o adversário, visando proteger a vida humana e a destruição das propriedades (DEPARTMENT OF DEFENSE, 2015).

O governo dos Estados Unidos tem realizado esforços no intuito de defender sua nação contra ameaças cibernéticas, de forma eficaz, e, nesse processo, o USCYBERCOM demonstra ser um comando fundamental para elevar o nível de proteção das redes governamentais e militares, pois orienta como o serviço militar deve treinar, equipar e comandar suas forças para a missão cibernética (LYNN III, 2010).

2 A GUERRA CIBERNÉTICA NAS FORÇAS ARMADAS DOS ESTADOS UNIDOS

Devido à emergência do ciberespaço em assuntos estratégicos na segurança internacional, cada vez mais se mostra importante que os Estados se organizem de forma que possibilite a defesa e liberdade de atuação nesse espaço. Para isso, os EUA designaram unidades para apoiassem o USCYBERCOM, entre elas a Força Aérea, Marinha e Exército, isto é, tendo assim suas unidades que possam operar na guerra cibernética.

2.1.1 Comando Cibernético da Força Aérea (AFCYBER)

Em dezembro de 2005, o Secretário da Força Aérea estadunidense Michael W. Wynne e o Chefe do Staff General T. Michael Moseley revelaram a nova missão em *statement* para os a Força Aérea dos Estados Unidos: "Deve oferecer opções soberanas para a defesa dos Estados Unidos da América e seus interesses globais – voar e lutar no ar, no espaço e no ciberespaço" (AFCYBER, 2014).

A nova atribuição de missão destacou a emergência de assuntos relacionados às operações cibernéticas, e a Força Aérea dos EUA reconheceu militarmente tal domínio. Dessa maneira, também é exposto que esta declaração de missão marcou o início de um processo que levaria o estabelecimento da 24ª Força Aérea, que representaria uma organização capaz de conduzir a gama de missões cibernéticas da Força Aérea norte-americana e que também forneceria forças de combatentes de apoio para as operações militares (AFCYBER, 2014).

Em agosto de 2009, o Comandante do Comando Espacial da Força Aérea (AFSCPC) General C. Robert Kehler presidiu a cerimônia de atuação da 24ª Força Aérea na base de Lackland, no Texas. Ainda o general assumiu o comando da nova organização que incluía o *staff* da sede, o 624º Centro de Operações, a 67ª Ala de Rede de Guerra (NWW) e o recém-criado 688º Esquadrão de Operações de Informação. Durante a cerimônia de ativação, o General expôs que:

> Hoje é verdadeiramente um dia histórico para a nossa Força Aérea. A ativação de 24ª Força Aérea continua a evolução do compromisso da Força Aérea de "Voar, Lutar e Vencer no Ar, no Espaço e no Ciberespaço". Nós movemos nossas capacidades cibernéticas sob o Comando Espacial da Força Aérea como comando principal, continuando a evolução cibernética como uma potente capacidade de

> combate à guerra. A 24ª Força Aérea demonstra ainda o compromisso da Força Aérea em apoiar os objetivos do DoD no ciberespaço. Pela primeira vez na história da Força Aérea, consolidamos as capacidades cibernéticas sob um combatente operacional dedicado exclusivamente a operações cibernéticas (AFCYBER, 2014, tradução nossa).

Como missão, a 24ª Força Aérea elucida "operar, estender e defender a rede de informação da Força Aérea e a missão principal sistemas, bem como fornecer recursos de espectro completo para o Combatente Conjunto, via ciberespaço" (AFCYBER, 2014, tradução nossa).

Seguindo sua ativação, os membros da 24ª Força Aérea trabalharam na perspectiva de obter certificação e capacitação operacional plena. A capacidade operacional foi iniciada no dia 22 de janeiro de 2010 e a certificação foi obtida no mesmo ano. Após isso, a 24ª Força Aérea passou a empregar o comando e controle limitado de forças cibernéticas ao USCYBERCOM (AFCYBER, 2014).

Em 2011, a 24ª Força Aérea continuou a ajustar a estrutura organizacional e assumiu seu papel como autoridade de comando e controle de nível operacional para forças cibernéticas. A sede contava com 206 oficiais, entre eles membros alistados e civis. O Centro de Operações continha mais de 4000 membros (AFCBYBER, 2014).

Neste mesmo ano, o General Webber foi para a reserva e a major-general Suzanne M. Vautrinot assumiu o comando da 24ª Força Aérea. Vale ressaltar que a general Valtrinot possui vasta experiência em operações cibernéticas, pois já tinha desempenhado a função de Diretora de Planos e Política do USCYBERCOM. Ainda pode-se afirmar que a diretora continuou a desenvolver a organização para operacionalizar e normalizar as operações cibernéticas da Força Aérea. Além disso, encaminhou e possibilitou melhorias para as forças cibernéticas, como também o desenvolvimento de comando operacional para apoiar a Força Aérea dos EUA (AFCYBER, 2014).

2.1.2 Comando Cibernético da Marinha e das Forças dos Fuzileiros Navais dos EUA (MARFORCYBER)

A respeito da Marinha dos Estados Unidos, é notado que a mesma teve de se organizar para poder desenvolver suas capacidades no espaço cibernético e operar de forma funcional. Mais uma vez, percebe-se, aqui, o desejo dos militares norte-

americanos em dominar o espaço cibernético. É observada também a presença de Frotas em diversas partes do mundo, como a 5ª Frota que navega no Golfo Árabe, a 6ª Frota no Mediterrâneo e a 7ª no Mar da China. Tendo em vista a guerra cibernética, a Marinha dos EUA reativou sua 10ª Frota. No que tange a esta última, a mesma era uma pequena organização que durante a 2ª Guerra Mundial comandava a guerra antissubmarino e logo após foi dissolvida com o término do conflito. Para aproveitar e capacitar a 10ª Frota, o Comando Naval de Guerra e Redes (NETWARCOM) terá responsabilidades operacionais sob a 10ª Frota (CLARKE; KNAKE, 2015).

Desse modo, pode ser evidenciada uma série de missões por parte do Comando do Ciberespaço das Forças dos Fuzileiros Navais dos EUA (MARFORCYBER). Uma das missões se configura da forma em que o Comandante do Comando do Ciberespaço Das Forças do Corpo de Fuzileiros Navais (COMMARFORCYBERCOM) e como o comandante do componente do Corpo de Fuzileiros Navais para o Comando Cibernético dos EUA (CDRUSCYBERCOM) tem a responsabilidade de representar as capacidades e interesses do Corpo de Fuzileiros Navais. Ainda aconselha o CDRUSCYBERCOM no que diz respeito ao uso adequado e apoio das forças do Corpo de Fuzileiros Navais, que coordena a implantação, emprego e planejamento de atividades ligadas às forças (MARFORCYBER, 2018).

Como outra missão da Marinha americana diz respeito ao COMMARFORCYBERCOM consentir operações no ciberespaço de total espectro, incluindo o planejamento das Operações de Rede Empresarial do Corpo de Fuzileiros Navais (MCEN Ops). Assim, as Operações Defensivas do Ciberespaço (OCO) com do Corpo de Fuzileiros Navais, Forças Conjuntas e de Coalizão planejam e quando autorizada a direção das operações ofensivas no ciberespaço em apoio às Forças Conjuntas de Coalizão, com o intuito de permitir a liberdade de ação em todos os domínios da guerra e negar o mesmo para forças adversárias (MARFORCYBER, 2018).

Sobre aspectos operacionais do MARFOCYBER, o COMMARFORCYBERCOM detém controle operacional do Grupo de Guerra do Ciberespaço do Corpo de Fuzileiros Navais (MCCYWG) e do Grupo de Operações do Ciberespaço do Corpo de Fuzileiros Navais (MCCOG) para apoiar os requisitos e tarefas da missão. Além disso, o COMMARFORCYBERCOM exerce papel de Comandante da Sede da Força Conjunta Cibernética (JFHQ-C)/ Marinha (JFHQC-C). O JFHQ-C da Marinha fornece suporte aos Comandos Combatentes para Operações Ofensivas no Ciberespaço (OCO) e, quando coordenado, realiza operações no

ciberespaço através de forças cibernéticas relacionadas. A JFHQ-C da Marinha tem como responsabilidade o comando, controle e gerenciamento das forças relacionadas ao ciberespaço (MARFORCYBER, 2018).

Ainda observando a forma com que o MARFOCYBER opera, é notada uma divisão entre o mesmo, isto é, o Comando do Ciberespaço das Forças dos Fuzileiros Navais dos EUA possui uma série de unidades e subunidades ligadas a esse comando. Uma delas é o Grupo de Operações do Ciberespaço do Corpo de Fuzileiros Navais (MCCOG), que tem como função executar Operações do Departamento de Defesa do Corpo de Fuzileiros Navais e Operações do Ciberespaço Defensivo do Corpo de Fuzileiros Navais (DCO) para que possa ser ampliada a liberdade de ação nos domínios de guerra, negando os esforços dos adversários no ciberespaço para com os EUA (MARFORCYBER, 2018).

No tocante às principais tarefas exercidas pelo MCCOG, é evidenciado o fornecimento de suporte de operações no ciberespaço para Forças-Tarefas Aéreas-Terrestres-Marítimas (MAGTFS), assim como planejar e direcionar as operações da Rede Empresarial do Corpo de Fuzileiros Navais (MCEN). Além disso, é visto um planejamento de Operações Defensivas Diretas no Ciberespaço (MARFORCYBER, 2018).

Outra subunidade que o MARFOCYBER possui é o Grupo de Guerra do Ciberespaço do Corpo de Fuzileiros Navais (MCCYWG), que tem o papel de organizar, treinar, equipar, fornecer suporte administrativo e gerenciar equipes da Força Missão Cibernética (CMF) e do USCYBERCOM. Ainda sob orientação do COMMARFORCYBER, a subunidade fornece dá suporte em serviços requisitados, comando combatente e coalizão (MARFORCYBER, 2018). A seguir, é demonstrada a Tabela 1, com as principais atividades desempenhadas pelo MCCYWG.

Tabela 1 Atividades desempenhadas pelo MCCYWG

1.	Conduzir questões de gestão de pessoal para melhor organizar e designar pessoas para funções de trabalho e colocá-los preparados para operações das equipes de CMF.
2.	Garantir treinamento de acordo com os Padrões Conjuntos de Treinamento e Certificação em Ciberespaço do USCYBERCOM e equipamento para executar atividades na Lista de Tarefas Essenciais da Missão MARFORCYBER (METL).
3.	Planejar e, quando autorizado, conduzir OCO, incluindo a investigação de redes, Inteligência Cibernética, vigilância e reconhecimento e preparação operacional do ambiente.
4.	Aconselhar o COMMARFORCYBER sobre considerações de emprego da força.

5.	Fornecer equipamentos especializados para os requisitos de planejamento operacional.
6.	Operar no ciberespaço são executadas através de três equipes de missão de combate, oito equipes de proteção cibernética e uma equipe de suporte cibernético, fornecendo apoio aos requisitos do Corpo de Fuzileiros Navais e da Força Conjunta.

Fonte: Elaboração própria baseada em MARFOCYBER (2018).

A Marinha ainda detém operadores responsáveis por uma variedade de tarefas para incluir operações cibernéticas defensivas, análise digital, análise de exploração e planejamento cibernético. A Marinha também possui técnicos de sistemas de informação que são responsáveis por realizar tarefas cibernéticas como operação e manutenção de sistemas globais de telecomunicações e redes locais e de longa distância, como também sistemas de microcomputadores usados na frota (POMERLAU, 2017).

2.1.3 Comando Cibernético do Exército (ARCYBER)

O Comando Cibernético do Exército (ARCYBER), estabelecido em 1 de outubro de 2010, é a linha de frente de defesa contra *hackers*, violação de dados e invasões de rede. O Comando também é responsável por manter e desenvolver superioridade tecnológica em meio a mudanças de ameaças em que o ciberespaço e a tecnologia podem apresentar-se (ARMY CYBER, 2017).

O ARCYBER é um elemento de serviço do USCYBERCOM e apresenta dois principais comandos subordinados: o 9º Comando de Sinal, tendo como função manter e defender a rede de computadores para permitir a superioridade da informação e garantir a operação, gerando acesso à rede de todas as fases da operação; e o 1º Comando de Operações de Informação, que tem como função principal o fornecimento de suporte aos comandos do Exército para planejamento e execução de Operações de Informações (LIEB, 2013).

Em aspectos de missão, o ARCYBER é responsável por "dirigir e conduzir operações integradas de guerra eletrônica, informação e ciberespaço como autorizadas ou dirigidas para assegurar a liberdade de ação no ciberespaço e no ambiente de informação, e negar o mesmo a nossos adversários" (ARCYBER, 2018, tradução nossa).

Desse modo, ainda acerca do papel desempenhando pelo ARCYBER, o comando é responsável por uma série de atividades, tais como:

Tabela 2 Responsabilidades da Missão Cibernética do Exército dos Estados Unidos da América

1.	Monitorar ininterruptamente ameaças cibernéticas e vigiar por tempo integral as redes globais do Exército.
2.	Trabalhar com o Exército, agências conjuntas e parceiros da indústria visando a superioridade do desenvolvimento e capacitação tecnológica no ciberespaço.
3.	Modernizar redes e melhorar as operações defensivas no ciberespaço.
4.	Criar suporte à rede do ciberespaço no nível do corpo de Exército incluindo unidades de combate.
5.	Recrutar, desenvolver e gerenciar profissionais capazes de atuar no ciberespaço.
6.	Promover recursos cibernéticos ofensivos e defensivos para combater ameaças maliciosas.
7.	Modernizar as redes e, assim, fornecer sistemas de combate resilientes do Exército para enfrentar desafios em qualquer ambiente operacional.

Fonte: Elaboração própria, baseada em ARCYBER (2018).

Neste intento, é importante destacar que as organizações militares exigem componentes semelhantes para cumprir sua finalidade (LIEB, 2013). Essas organizações demandam estruturas, pessoas, ativos e outros componentes que são necessários para a realização da missão, além de requerer alinhamento e sincronização entre os componentes para facilitar suas atividades (LIEB, 2013).

Atualmente, a ARCYBER realiza duas missões em dois locais diferentes. Uma das missões defende as redes do Exército por meio de unidades de sinalização operando sob o Comando de Tecnologia Empresarial da Rede do Exército dos Estados Unidos (NETCOM), que lidera as operações globais na porção do Exército e que garante liberdade de ação no ciberespaço, enquanto é responsável também de negar as atividades a adversários. A segunda missão é o preparo ofensivo para com as redes adversárias mediante unidades do Centro de Inteligência e Comando (ISCOM) operando sob a tutela da Agência de Segurança Nacional (NSA). Vale ressaltar que as unidades de operação NETCOM e INSCOM possuem também seu próprio comando e controle (LIEB, 2013).

Os soldados do NETCOM são atribuídos a um batalhão de sinais, que faz parte de um Centro de Operações de Segurança de Redes de Teatro (TNOSC). O TNOSC é responsável pelo gerenciamento de rede e defesa de computadores do Exército, sendo um teatro funcional específico de operações. O INSCOM é responsável pela Inteligência de Sinais (SIGINT) para apoiar o Exército. Os soldados do INSCOM gerem a SIGINT em atividades que primeiramente são desempenhadas pelas instalações da NSA (LIEB, 2013).

Diante disso, o Exército formou seu primeiro batalhão de guerra em redes

(ANWB) e designou soldados para desempenhar trabalho em centros da NSA, para condução de atividades cibernéticas. O Exército criou a 780th MI Brigade, que é conhecida como Cyber Brigade, e a ANWB tornou-se a 781th MI Brigade, em outubro de 2011. Ainda a respeito dessa organização estrutural, o Exército formou o segundo batalhão 782nd, no Forte Gordon, na Geórgia. Sobre seu financiamento, é possível afirmar que o 780th MI Brigade é financiado pelo Exército, e não pela NSA. As forças apresentadas estão sob o controle operacional de ARCYBER, e não da NSA. Mesmo que a NSA não seja responsável pelo financiamento, ela ainda possui o papel de dar direcionamento em atividades cibernéticas (LIEB, 2013).

A Tenente-Coronel Lieb (2013), no que tange à estrutura organizacional, elucida que se deve alinhar orçamento, missão, direção e autoridades. Esse alinhamento adequado pode representar avanços nas unidades de comando e de esforço, resultando em operações cibernéticas defensivas e ofensivas com um maior nível de sincronização que possam ser comandadas por sedes funcionais (LIEB, 2013). A Coronel aponta que no domínio cibernético é necessária uma maior agilidade de tomada de decisão que só pode ser obtida com um esforço unificado. É apresentado, ainda, que o Exército deve procurar organizar-se e designar o ARCYBER como um componente de serviço do Exército (ASCC) sob o USCYBERCOM (LIEB, 2013).

2.2 Criação do Comando Cibernético (USCYBERCOM)

Com a rapidez e agilidade com que a informação tem se propagado, em decorrência da Revolução da Informação, gradualmente são apresentados desafios aos Estados no que tange à forma de organizar suas instituições em assuntos relacionados à segurança cibernética. Nesse intento, o USCYBERCOM se demonstra como uma alternativa em proteção de redes governamentais e militares.

Devido à atitude progressista da Força Aérea norte-americana em aspirar ao papel de liderança no ciberespaço, em 23 de junho de 2009, o Departamento de Defesa dos Estados Unidos estabeleceu um comando subunificado[10], o USCYBERCOM, localizado em Forte Mead, no Estado americano de Maryland. O quartel-general coordena esforços no DoD de combater ameaças e garantir liberdades no espaço cibernético. Parte do orçamento de Defesa é dedicada ao USCYBERCOM, devido à

[10] Subunificado significa abaixo do Comando Estratégico dos Estados Unidos (USSTRATCOM).

importância emergente do ciberespaço (GRAHAM, 2016).

Tendo como papel pioneiro na defesa cibernética em combater intrusões em tempo real, a NSA estabeleceu sistemas de sensores, como também agentes responsáveis pela defesa e melhor projeção de ações no campo cibernético, o que representou uma mudança na forma com que os EUA defendiam suas redes. Além disso, o país colocou a tecnologia de digitalização na interface das redes militares e também na Internet, com o propósito de identificar possíveis ameaças, antes de passá-las por redes militares. Desse modo, uma defesa ativa tem representado a consolidação de capacidades de defesa cibernética por parte do DoD, sendo um dos motivos para que pudesse ser criado o USCYBERCOM (LYNN III, 2010).

Anteriormente à data de criação do USCYBERCOM, nos anos 1990, podia ser observado certo nível de mobilização por parte da Força Aérea em desenvolver ferramentas eficazes para combater possíveis conflitos no ambiente cibernético. Nessa mesma época, ainda não existia um completo entendimento da guerra cibernética, isto é, era comum pensá-la como "operações de informação" ou como "operações psicológicas". Além do mais, começou-se a notar que, caso acontecesse alguma invasão em certa rede de dados, seria possível destruí-la. Também era possível observar o surgimento de um dilema entre *geeks* e operadores de unidades de combate, pelo fato de a Internet estar se transformando em um campo de batalha, e que o compartilhamento de informações poderia fazer com que perdesse o controle do ciberespaço para esses combatentes, o que representaria uma perda de possíveis lucros, posto que nessa época aconteceu uma ascensão da espionagem eletrônica (KNAKE; CLARKE, 2010).

No segundo mandato do presidente George W. Bush, a guerra cibernética ganhou valor significativo para o Pentágono. Desta forma, houve uma mobilização da Força Aérea e da Marinha, junto com agências de Inteligência, para ver quem iria estar à frente desse novo tipo de guerra. Foi dada ao Comando Estratégico (USSTRATCOM) [11] responsabilidade sobre a guerra cibernética. Havia uma preocupação em manter a existência da capacidade da guerra cibernética em sigilo, mesmo que a Força Aérea falasse abertamente sobre o assunto. Como posto por Clarke e Knake (2015), isso pode ser evidenciado no discurso do Secretário Civil da Força Aérea que declarou publicamente que "estamos na era da Guerra Cibernética", como

[11] Estabelecido em 1 de outubro de 2002, o USSTRATCOM é responsável pela dissuasão estratégica e operações na rede global de informações. Além disso, fornece recursos que dão suporte a outros comandos combatentes, incluindo defesa integrada de mísseis, comando global, controle, comunicações, computadores, Inteligência, vigilância e reconhecimento (C4ISR).

também no discurso do diretor da Força de Tarefa de Operações no Ciberespaço da Força Aérea, de que "nossa missão é controlar o ciberespaço, tanto para ataque quanto para defesa" (KNAKE; CLARKE, 2010, p. 34, tradução nossa).

Por conseguinte, no que concerne à missão do USCYBERCOM é possível entender que ele:

> planeja, coordena, integra, sincroniza e conduz atividades para: direcionar as operações e a defesa de determinadas redes de informação do Departamento de Defesa; prepara-se, quando dirigido, para conduzir operações espaciais no ciberespaço em todo o espectro para permitir ações em todos os domínios, garantir a liberdade de ação dos EUA/aliados no ciberespaço e negar o mesmo aos adversários (DEPARTMENT OF DEFENSE, 2010, tradução nossa).

Ainda observando as atividades primordiais do USCYBERCOM, no que tange às áreas em que o USCYBERCOM deve ter enfoque, já que o Comando deve atuar em três principais áreas, a saber: Rede de Informação do Departamento de Defesa (DoDIN); fornecimento de suporte aos combatentes nas mais variadas missões ao redor do mundo; e viabilizam a capacidade dos EUA em responder e resistir a ataques cibernéticos. Além disso, o comando sobre as operações do ciberespaço elucida que:

> Unifica a direção das operações do ciberespaço, fortalece as capacidades do ciberespaço do DoD e integra e reforça a experiência cibernética do mesmo. O USCYBERCOM melhora as capacidades do DoD em operar redes de informação e de combater ameaças do ciberespaço, procurando garantir seu sucesso. O USCYBERCOM está projetando a estrutura da força cibernética, ou seja, tratando dos requisitos de treinamento e dos padrões de certificação que permitirão que os serviços tenham a força cibernética necessária para executar as missões atribuídas. O comando também trabalha em estreita colaboração com parceiros interagências e internacionais na execução dessas missões críticas (DEPARTMENT OF DEFENSE, 2010, tradução nossa).

No que tange às missões do USCYBERCOM, é possível observar a proteção cotidiana de todas as redes de defesa e também apoiar missões militares no ciberespaço. A segunda é a possibilidade de fornecer e organizar os recursos necessários para uma guerra cibernética de todo o Exército, na formação e fornecimento de soldados. Desse modo, ainda o USCYBERCOM é responsável por supervisionar os comandos dentro de cada ramo das Forças Armadas, dentre eles, a *Army Forces Cyber Command*, a 10ª Frota da Marinha dos EUA, a 24ª Força Aérea e as Forças do Corpo de Marines do

Comando do Ciberespaço[12], da forma em que as forças operacionais possam funcionar em um ambiente em que seja difícil a transferência de informações. Na terceira missão, por sua vez, o USCYBERCOM deve trabalhar com parceiros que façam parte ou não do governo[13] dos EUA, como representantes do Federal Bureau of Investigation (FBI), Departamento de Justiça e Agência de Sistemas de Informação de Defesa, que também trabalham em Fort Mead. Além disso, o USCYBERCOM possui uma estreita colaboração com setores da indústria privada para compartilhar informações sobre ameaças (LYNN III, 2010).

Em complementação do que foi exposto por Lynn III (2010), Graham (2016) expõe que integrantes de todas as Forças Singulares estão reunidos no USCYBERCOM para operar contra possíveis ameaças no ciberespaço. Com base nos dados fornecidos pelo DoD, devido ao aumento das ameaças cibernéticas, foi solicitado cerca de 6,7 bilhões de dólares, que serão destinados a reforçar a defesa cibernética no ano de 2017, representando assim um aumento de quase 900 milhões de dólares em relação a 2016. O Comandante do USCYBERCOM, almirante Michael S. Rogers, em um painel da Câmara dos Deputados dos EUA, em março de 2017, ressaltou a importância de continuar os investimentos para com o enfretamento de ameaças cibernéticas avançadas. Assim, sobre o USCYBERCOM em operação, no seu testemunho, Rogers alega que, cada vez mais, o Comando tem rastreado adversários estatais e não estatais, devido ao contínuo desenvolvimento de capacidades na finalidade de garantir os interesses dos Estados Unidos e de seus aliados. À vista disso, é pertinente salientar que existe uma preocupação com o aumento de eventos relacionados a ataques cibernéticos pelas mais diversas partes do mundo. Em um discurso sobre, Rogers afirma que:

> Todos os conflitos em todo o mundo agora têm uma dimensão cibernética. “Guerra cibernética” não é um conceito futuro ou um espetáculo cinematográfico; é real e veio para ficar. O fato de você não matar pessoas ainda, ou causar destruição generalizada, não deve ser um consolo para nós. O conflito no domínio cibernético não é simplesmente uma continuação das operações cinéticas por meios digitais nem é um conflito de ficção científica de exércitos de robôs. Está se desenrolando de acordo com sua própria lógica, que continuamos a entender melhor. Estamos usando como compreensão para aprimorar a consciência situacional do DoD e gerenciar riscos. À luz desta tendência, estou convencido de que nós, como nação, criamos nossa própria capacidade militar no ciberespaço. Nosso governo e militares têm se preocupado em saber se nós temos um

[12] Componentes ligados à guerra cibernética.
[13] Um exemplo de parceria com empresa privada é a Sony Corporation, logo após os ataques cibernéticos sofridos da Coreia do Norte.

> problema sistêmico de segurança em computadores para reconhecer que o problema pode se espalhar em segundos (DEPARTMENT OF DEFENSE, 2017, p. 4, tradução nossa).

Seguindo esse painel, o Comandante Rogers ressalta que linhas de operações são para garantir missões do Departamento de Defesa e também defender o meio em que as informações são conduzidas pelo DoD; dar apoio aos objetivos comuns do comandante da força conjunta, para dissuadir ou derrotar ameaças estratégicas nocivas aos interesses dos EUA e sua infraestrutura crítica. Também, é pertinente a realização de operações militares no ciberespaço para permitir ações em todos os domínios, com o intuito de garantir aos EUA e aliados liberdade de ação no ciberespaço e negar a ação aos adversários (DEPARTAMENT OF DEFENSE, 2017).

Previamente, as autoridades do USCYBERCOM, em 24 de outubro de 2016, anunciaram que a Força Cibernética do Comando dos Estados Unidos (CMF) tinha atingido a capacidade inicial de atuação a partir dessa data. Formada por 133 equipes, a Força de Missão Cibernética compreende cerca de 5.000 indivíduos nessas equipes. A previsão para o ano de 2018, de acordo com o Departamento de Defesa, é aumentar para 6.200 indivíduos e que todas as 133 equipes estejam operando em sua totalidade. Devido ao desenvolvimento veloz e dinâmico do domínio cibernético, as equipes da Força da Missão Cibernética são responsáveis por salvaguardar a nação contra ataques cibernéticos (DEPARTMENT DE DEFESA, 2016)

As Forças de Missão Cibernética do USCYBERCOM se alinham com a estratégia do Departamento de Defesa. Ainda, os grupos da Força da Missão Cibernética são responsáveis por dar suporte às operações do Departamento e possuem suas próprias atribuições. As equipes que formam a Força Nacional de Missão Cibernética são responsáveis pela defesa da nação em uma atividade adversária. As equipes das Forças de Combate da Missão Cibernética têm o papel de conduzir operações cibernéticas militares em apoio aos comandos combatentes. Já as equipes da Força de Proteção Cibernética defendem as redes de informação e preparam as forças cibernéticas para o combate. Também fazendo parte dos grupos da Força de Missão Cibernética, as equipes de Suporte Cibernético fornecem apoio extensivo e de idealização às equipes da Missão Nacional e da Missão de Combatente (DEPARTMENT OF DEFENSE, 2016).

Com as observações de atividades no ciberespaço realizadas pela Força da Missão Cibernética do USCYBERCOM, foi constatado que atores não estatais, como o

Estado Islâmico, estariam desenvolvendo melhorias consideráveis em suas capacidades cibernéticas. Ademais, esses atores podem ter acesso a informações pessoais de cidadãos e também redes que controlam a infraestrutura do país. Assim, os adversários dos Estados Unidos estariam desenvolvendo operações que seriam capazes de limitar o campo de atuação dos EUA em determinados momentos de crise. Como ferramenta essencial na luta contra adversários no espaço cibernético, a construção da Força Cibernética seria de importância na manutenção da defesa dos interesses norte-americanos (DEPARTMENT OF DEFENSE, 2016).

Outrossim, pode se observar que atores estatais estão a ameaçar o espaço cibernético dos Estados Unidos. O Comandante Rogers postulou que a China e a Rússia continuam sendo classificadas como as maiores ameaças à segurança dos Estados Unidos, e também, regimes como o Irã e a Coréia do Norte tem ampliado suas aptidões em atividades no ciberespaço sem terem medo de continuar ampliando seus potenciais, despertando assim, um interesse maior dedicação em relação às abordagens e eficácias que podem ser adotadas pelo país para que possa proteger melhor seu ciberespaço (PEREZ, 2018).

No *House Armed Services Committee*, foi realizada uma audiência no dia 22 de junho de 2016, em que o Almirante General Moore destrincha sobre a natureza particular das operações e ameaças no ciberespaço criam diversos desafios para o Departamento de Defesa. Na audiência, foi dito que as capacidades de combate norte-americana estão mais confiantes do domínio cibernético, além de prever crescimento considerável a respeito das mudanças que podem acontecer no campo. Moore apontou que o Departamento de Defesa tem realizado melhorias significativas como a Força Missão Cibernética e, assim, se destina em oposição a um adversário de conseguir operar livremente no ciberespaço. Mesmo com melhorias consideráveis, o Almirante reafirma o compromisso com a Força Missão Cibernética relatando os progressos significativos realizados em todas as áreas no ano anterior e buscando equipar a força de forma eficaz, como também estabelecer um ambiente de treinamento contínuo, visando responder os possíveis desafios que devem surgir, ou seja, dando estrutura de comando e controle para a Força Missão Cibernética (DEPARTMENT OF DEFENSE, 2016).

Em fevereiro de 2018, foi anunciado que a sede da Joint Force DODiN, que é uma sede responsável pela segurança, operação e defesa da complexa infraestrutura de tecnologia de informação do Dod chegou no ponto pleno de suas capacidades de operações. Outra força ressaltada pelo Almirante foi a Força-Tarefa Conjunta Ares,

responsável para combater as forças do Estado Islâmico no Iraque e Síria, que, de acordo com ele, conseguiu "excelentes resultados". Com relação ao treinamento, o USCYBERCOM aumentou de forma considerável o preparo para com o campo de batalha contra seus principais adversários. Ademais, em seu anúncio, Rogers revelou que o USCYBERCOM iria se transofrmar em um centro cibernético integrado de última geração e juntar forças de operação a Fort Meade, em Maryland, aumentando a coordenação e o planejamento de operações contra ameaças cibernéticas. O foco do USCYBERCOM em inovação e desenvolvimento tecnológico também alcançou desde pequenos negócios até parcerias com o setor privado encarregado por manter a segurança cibernética (PEREZ, 2018).

No quarto exercício anual da Guarda Cibernética, realizado de 8 a 26 de junho em 2015, em Suffolk, no estado da Virgínia, participaram operadores de infraestruturas críticas do ciberespaço e especialistas de quase 100 organizações, além do governo, indústria e coalização internacional. Esse encontro foi realizado com o intuito de forjar parcerias militares, federais e com o setor privado, necessárias para o aperfeiçoamento da Guarda Cibernética[14]. O Almirante Rogers explicou que a Guarda Cibernética foi criada para exercitar a interface entre os componentes ativos e de reserva do Departamento de Defesa, com enfoque na missão cibernética, além de parcerias com outros componentes do governo dos EUA. Juntamente, a participação da indústria privada incluiu várias informações e centros de análises de compartilhamento. Demonstrando que parcerias com o setor privado são essenciais, Rogers clareou que a Guarda Cibernética beneficiou-se de capacidades do setor privado ligadas às do governo federal dentro do DoD. O almirante afirmou, ainda, que o desafio recorrente é reunir as capacidades de todos os participantes e atender as suas mais diferentes necessidades. No encontro, o Vice-Almirante da Guarda Costeira, Kevin Lunday, responsável pelos treinamentos e exercícios do Comando Cibernético dos EUA, relatou o aprendizado de que a Guarda Cibernética ofereceu ao USCYBERCOM. Mais uma vez, esforços com os setores privados foram evidenciados, pois, segundo Lunday, a infraestrutura mais crítica nos Estados Unidos é a área de tecnologia da informação, que é de propriedade do setor privado, além de confiar nesse setor quando houver um incidente ou ataque mais robusto na seara privada (DEPARTMENT OF DEFENSE, 2015).

[14] Exercício de nível tático em operações de defesa nacional no ciberespaço e no comando e controle de missões integradas entre o USSCYBERCOM e a NSA em um ambiente propício para treinamento cibernético.

Conforme o vice-almirante Lunday, os aliados dos Estados Unidos são de importância em operações combinadas, sendo estas operações inerentes de coalização. Reforçando o papel do encontro, Lunday explicitou que era necessário que se mantivesse um ambiente de treinamento intensivo em que as forças pudessem treinar em de forma realista e integral, e não apenas algumas vezes por ano, pois os cenários certamente concretizar-se-ão, sendo que o Departamento de Defesa estará pronto para superar tais desafios (DEPARTMENT OF DEFENSE, 2015).

2.3 Críticas ao funcionamento do USCYBERCOM

Nas Forças Armadas dos EUA, existe uma divisão de trabalho entre as Forças Singulares. Por exemplo, a Força Aérea concentra sua superioridade aérea, permitindo que o Exército se dedique mais à guerra terrestre e que a Marinha esteja apta a combater no ambiente marítimo. Desta maneira, com a emergência do ciberespaço como domínio independente, se faz necessário o estabelecimento de uma própria perícia militar (GRAHAM, 2016). De forma convergente à atual abordagem adotada pelo Departamento de Defesa, Graham (2016) elucida que "uma força cibernética independente pode proporcionar o nível necessário de concentração nas operações no ciberespaço" (GRAHAM, 2016, p. 73, tradução nossa). Consoante o estrategista, mesmo com diversas Forças Singulares sob comando do USCYBERCOM, problemas como a irregularidade dos papéis tradicionais de combates nos domínios físicos e esforços no espaço cibernético podem provavelmente desencadear resultados indesejados ou incoerentes. Ele ainda afirma que o estabelecimento de uma Força Cibernética independente, a exemplo da chinesa, permitiria, a comandantes com ampla experiência no ciberespaço, uma melhor comunicação nos desafios da guerra cibernética. Isto posto, os chefes da Força Cibernética poderiam fornecer eficientes orientação e recursos destinados às operações militares no ciberespaço. Juntamente, a formação de guerreiros cibernéticos poderiam ser um passo benéfico para proporcionar melhores operações no ciberespaço. Assim, é claro que a Força Cibernética poderia atrair e formar soldados mais qualificados (GRAHAM, 2016). O treinamento de guerreiros[15] é apontado como uma dessas melhorias na Força Cibernética, mesmo que atualmente cada Força Singular tenha seus treinamentos específicos, as interpretações

[15] Ou, como preferem Clarke e Knake, "guerreiros cibernéticos".

entre elas irão ficar desconectadas, mesmo que de forma bastante sutil. Em outras palavras, apesar de possuírem padrões comuns de treinamento, as interpretações podem ser diferentes e as habilidades variadas por partes dos instrutores podem produzir guerreiros cibernéticos de qualidade não requerida para a missão de qualidade inferior à ideal (GRAHAM, 2016).

Seguindo essa lógica, o benefício principal do estabelecimento de uma Força Cibernética independente seria a capacidade de desenvolver uma Força que fosse a mais apta possível, resultando em mais eficiência e menos riscos dentro do ciberespaço. Em diferenciação aos outros domínios, Graham (2016) declara que:

> Nos domínios físicos, é relativamente fácil dividir o campo de batalha por localização física: o Exército opera no interior, a Marinha no mar, os Fuzileiros Navais nos litorais e a Força Aérea no céu. No entanto, não existem essas fronteiras óbvias no ciberespaço, e todas as quatro Forças Singulares atuam por todo ele. A oportunidade de uma Força Singular infringir ou sabotar inadvertidamente uma operação cibernética de outra é muito maior do que nos domínios físicos separados. O ônus de comando e controle e o risco de fratricídio no ciberespaço aumentam com o número de guerreiros cibernéticos das quatro Forças Singulares diferentes atuando independentemente no domínio. Outra consequência de quatro distintos esforços no ciberespaço é o potencial de redundância não intencional (*i.e.*, duas Forças Singulares podem dedicar recursos para resolver o mesmo problema ou desenvolver a mesma capacidade). Um esforço conjunto de supervisão pode reduzir um pouco da redundância, porém mais burocracia acrescenta tempo e custos a um processo de desenvolvimento de capacidade já demorado. A remoção das quatro Forças Singulares do combate pelo ciberespaço reduz o risco de elas pisotearem umas às outras e de desperdiçar recursos. (GRAHAM, 2016, p. 75-76, tradução nossa).

Uma abordagem ainda mais ambiciosa e diferente da atual, seria a elevação do USCYBERCOM para o mesmo nível do USSTRATCOM. Para Graham (2016), essa elevação representaria um passo importante no intuito de estabelecer uma Força Cibernética independente. O estrategista alega que poderia eliminar as camadas hierárquicas do USCYBERCOM e os formuladores de políticas. Pertinente à elevação do USCYBERCOM, em 18 de agosto de 2017, o Presidente Donald Trump Jr., em um *statement*, anunciou que o Comando Cibernético dos Estados Unidos fosse elevado ao *status* de um Comando Unificado de Combatentes, que seria focado a operações no ciberespaço. No *statement* o presidente anunciou que:

> Este novo Comando Unificado de Combatentes fortalecerá nossas operações no ciberespaço e criará mais oportunidades para melhorar a defesa de nossa nação. A elevação do Comando Cibernético dos Estados Unidos demonstra nossa crescente determinação contra as ameaças do ciberespaço e ajudará a tranquilizar nossos aliados e

> parceiros e deter nossos adversários. A elevação do Comando do Ciberespaço dos Estados Unidos também ajudará a simplificar o comando e controle de operações do ciberespaço sensíveis ao tempo, consolidando-as sob um único comandante, com autoridade compatível à importância de tais operações. A elevação também garantirá que as operações críticas do ciberespaço sejam adequadamente financiadas (WHITE HOUSE, 2017, tradução nossa).

Prévia a essa decisão do Presidente Trump, o *Government Accountability Office* (GAO), órgão responsável por reunir informações e ajudar o Congresso a avaliar as atividades do Executivo, lançou um *report* que examina as perspectivas no que tange às vantagens e desvantagens de uma liderança (*dual-hat*[16]) compartilhada entre a NSA e o USCYBERCOM. As vantagens apontadas por oficiais do Departamento de Defesa foram em direção a uma maior coordenação e colaboração entre a ambos os órgãos, mais rapidez no processo de tomada de decisão e uso mais eficiente dos recursos orçamentários cibernéticos. Em contrapartida, as desvantagens seriam prioridades que o USCYBERCOM receberia em relação a outros comandos, o que poderia causar problemas, já que a NSA é uma agência de apoio a comandos combatentes. Outra desvantagem apontada seria uma potencial exposição de ferramentas e operações da Agência. Os oficiais alegam que, ao compartilhar ferramentas, aumentaria o risco, devido à exploração e à obtenção de acessos a redes adversárias para fins de Inteligência. Por fim, poderia criar tensões entre as operações militares e ações de Inteligências, entre a Agência e o Comando Cibernético, visto que nem sempre poderiam concordar da forma de atuação de determinado problema (GOVERNMENT ACCOUNTABILITY OFFICE, 2017).

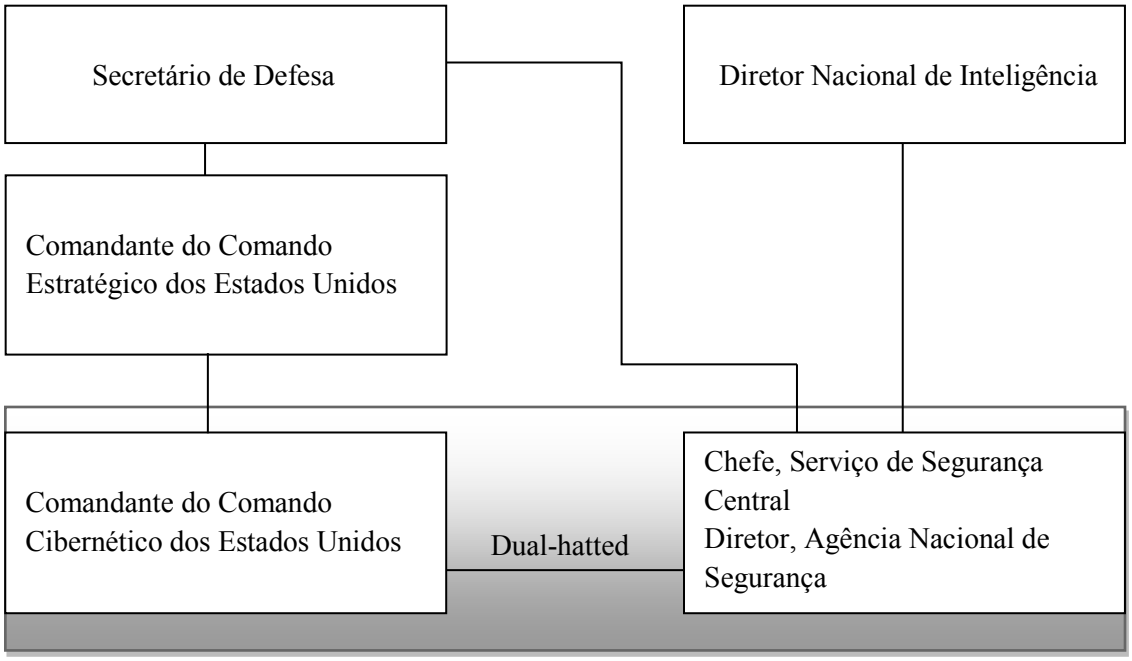
As recomendações do GAO são no sentido de o Departamento de Defesa tomar decisões para alterar seus critérios e definir as tarefas da Estratégia Cibernética do Departamento de Defesa. Outra recomendação é que deva estabelecer um cronograma de monitoramento para implementação de um objetivo da Campanha de Segurança Cibernética do DoD para o comandante em prontidão e responsável pelas avaliações de risco operacional. No *report*, é evidenciado que o Departamento de Defesa concordou com estas recomendações e que planeja realizá-las (GOVERNMENT ACCOUNTABILITY OFFICE, 2017).

A seguir, uma versão simplificada de tabela apresentada pelo GAO sobre os

[16] Nesse caso, o significado se refere à liderança compartilhada.

papéis e responsabilidades de um líder *dual-hatter* da NSA, do Serviço de Segurança Central (CSS) e do Comando do USCYBERCOM.

Figura 1 Organograma de Liderança para NSA, CSS e USCYBERCOM



Fonte: Elaboração própria, a partir de DoD (2017).

O Diretor da NSA é o líder do governo dos EUA para criptografia, além de ser o conselheiro principal do Departamento de Defesa em assuntos de Inteligência. Além disso, fornece assistência técnica para garantia da informação do Departamento de Defesa aos demais clientes nacionais. O Chefe de Serviço de Segurança Central promove uma parceria entre a NSA e elementos criptológicos das Forças Armadas. Por sua vez, o Comandante do USCYBERCOM defende funções críticas no ciberespaço contra invasões ou ataques, além de proteger informações da Pasta de Defesa. Ademais, está à frente de operações no ciberespaço, mantendo contato com outros departamentos e agências do governo norte-americano. É importante salientar que realizam operações cibernéticas com o intuito de garantir a negação de ataques inimigos, como também proteger suas próprias infraestruturas (GOVERNMENT ACCOUNTABILITY OFFICE, 2017).

Nesse intento, vale destacar conceitos como Exploração de Redes de Computadores (CNE) e Ataque a Redes de Computadores (CNA). De acordo com *Congressional Research Service Reports* de 2007, a CNE é uma área de informação de operações que ainda não estão claramente definidas no DoD. Desse modo, o

Departamento procura preparar o espaço de combate de informação de operações via Inteligência, vigilância e reconhecimento. Já o CNA pode ser definido como operações para interromper ou destruir informações residentes em computadores e redes de computadores. Além disso, a CNA depende de uma rede de dados usada como arma para executar o ataque. É importante ressaltar que ferramentas utilizadas para CNE são semelhantes às utilizadas pela CNA, mas são configuradas mediante coleta de Inteligência, em vez de interrupção do sistema (WILSON, 2007).

3 ESPAÇO CIBERNÉTICO COMO DOMÍNIO DE OPERAÇÕES: DESAFIOS AOS ESTADOS UNIDOS

3.1 Espaço cibernético como domínio de operações

De acordo com Libicki (2012), as operações cibernéticas ofensivas pretendem explorar falhas mínimas apresentadas pelos sistemas de informação, desse modo podendo criar efeitos que possam interferir na capacidade de transporte de informações de tarefas militares ou outras atividades como produção. Como evidenciado pelo autor, a respeito do funcionamento dessas tarefas, pode-se afirmar que "quanto mais estas tarefas requerem o funcionamento correto dos sistemas, maior é o potencial de interrupção ou corrupção que pode ser causado por adversários" (LIBICKI, 2012, p. 323). Em contrapartida, é elucidado que quanto mais rigoroso for o controle de informação, menor é o risco de ameaça que esses sistemas de informação vão enfrentar (LIBICKI, 2012).

Em relação aos meios de combate, pode-se afirmar que a maneira mais comum de causar uma intrusão se deve ao fato de que um sistema de informação está conectado a outros sistemas, isto é, quase todos os sistemas de informação são conectados à Internet, que basicamente é equivalente ao ciberespaço, pois tudo que está conectado à Internet está, necessariamente, ligado ao ciberespaço (LIBICKI, 2012).

Sobre a capacidade das FFAA nos quatro domínios, em comparação com o ciberespaço, Libicki (2012) elucida que:

> Uma coisa é reconhecer que a capacidade das forças armadas avançadas para realizar missões nos quatro domínios requer que eles sozinhos possam comandar seus sistemas. Outra é fundir o epifenômeno da conectividade à Internet de tais sistemas militares com a preposição de que o ciberespaço é um meio militar sujeito a princípios de guerra que existem em outros meios físicos. (LIBICKI, 2012, p 324, tradução nossa).

É de conhecimento geral que o ciberespaço é uma cria humana. Isso o torna diferente dos outros domínios. Não é apenas a natureza desse espaço que o torna diferente, mas a forma como ele se comporta, *i.e.*, altamente maleável (LIBICKI, 2012).

Levando em consideração essa maleabilidade do ciberespaço, os militares dos

EUA têm uma necessidade real de moldar seus sistemas de informação, pelo fato de estar sempre enfrentando inimigos capacitados a impedir que suas funções se tornem inoperantes, principalmente em períodos de conflito. Dessa maneira, os inimigos estão mais predispostos a utilizarem os computadores militares para realizar seus objetivos. No caso norte-americano, cada vez mais o Departamento de Defesa está disposto a fazer melhorias e investimentos que garantam que seu sistema não seja seriamente prejudicado por ações inimigas. Ainda, o DoD possui seu próprio domínio de Internet que executa com seu próprio servidor *web*. O Departamento também adquiriu grande parte do código-fonte do Microsoft Windows para que possam ser realizadas mudanças em recursos de segurança. Como apresentando, o ciberespaço é composto por múltiplas mídias e é maleável de diversas formas em que seus proprietários e operadores possam adquirir vantagens sobre seus oponentes (LIBICKI, 2012).

Sistematicamente, os militares dos EUA tornaram-se dependentes de tecnologias para dominar os campos de batalha (GARTZKE, 2013). No entanto, Gartzke (2013) elucida que a internet é geralmente um substituto inferior para a força terrestre em desempenhar funções de coerção e conquista. Além disso, a guerra cibernética não é provável para servir de árbitro final na concorrência em um mundo anárquico e assim não e deve ser considerado como uma das formas tradicionais de violência. Dessa maneira, Gartzke (2013) afirma que a falta de informação sobre os desenvolvimentos transformacionais ou meramente incrementais podem orientar quando o pânico está em ordem, quando não está. Mesmo em sociedades mais seguras, os indivíduos, grupos e comunidades estão sujeitos a uma varidade de perigos potenciais. Muito poderia ser feito para prejudicar esses indivíduos, mas são poucas as possibilidades que são realmente exercidas e experimentadas (GARTZKE, 2013).

A respeito da Internet, Gartzke (2013) possibilitou a interação com pessoas em qualquer lugar, e que a atenção inicial do ciberespaço se concentrou potencialmente para o bem, mas as conveniências também foram utilizadas para fazer conflitos. O fornecimento de alvos para atos cibernéticos de agressão é certamente enorme em relação à oferta de criminosos em violência física (GARTZEK, 2013, p. 11). À vista disso, é claro que o ciberespaço não é um domínio predominantemente de fraude, roubos de identidade e outros atos de predatórios. Outras tentativas casuais são utilizadas para prejudicar o bem-estar das pessoas, mas é com a mesma causalidade que podem ser ignoradas pelas maiores de site de spam ou *softwares* de marketing encontrados na Internet. É notório que grande parte das fraudes realizadas na internet e

da violência no ciberespaço estão ligados com o domínio físico, porque com o dano iniciado na internet, eventualmente pode ser perpetuado em formas mais convencionais (GARTZKE, 2013).

É de conhecimento geral que as nações e organizações podem ser atacadas via internet como as mesmas podem ser atacadas em espaço físico. Gartzke (2013) a respeito do espaço físico utiliza autores como Hensel (2000) e Senese (2005) que afirmam o protagonismo do espaço físico como o único preditivo de conflitos interestaduais é a proximidade de fronteiras. Em contrapartida, os ataques cibernéticos podem se manifestar como atos políticos apenas na medida em que eles influenciam a capacidade de afetar a tomada de decisões das organizações e soberanos (GARTZKE, 2013).

Libicki (2012) acredita que ao chamar ciberespaço de um domínio e guerra também promove a vontade de esboçar conceitos de guerra que são utilizados em domínios anteriores como terra, mar e ar. As noções do ciberespaço como um terreno de dominância não possuem o mesmo significado que os outros domínios. É possível questionar se o ciberespaço se apresenta como domínio devido às regras atuais de engajamento para combate cinético, pois as forças dos EUA estão autorizadas a disparar de volta quando estiverem sob ataques. É necessário salientar que essa doutrina apresenta alguns problemas substanciais, devido ao fato de supor que o ciberespaço pode apresentar uma força oposta à aquele que está supostamente capacitado para desarmar e destruir. Diante desse contexto, por exemplo, os hackers não podem ser destruídos por um ataque cibernético, implicando assim em um desarmamento de suas capacidades (inteligência, computadores e redes) pois as mesmas não podem ser destruídas por um ataque cibernético (LIBICKI, 2012).

A união do ciberespaço como um domínio representa expectativas para que o DoD, com o USCYBERCOM protejam o ciberespaço da mesma maneira que o Exército, Marinha e Aeronáutica protegem seus domínios. É colocado em questão se os Estados Unidos estariam protegidos contra ataques hostil nesse domínio, mas é sabido que o governo tem formulado um programa chamado Einstein III, que está sendo implementado para defender os domínios do governo em pontos críticos de sua infraestrutura e de sua base industrial de defesa. Esse programa ficaria conectado entre a Internet e as redes protegidas inspecionando *malwares* (LIBICKI, 2012).

Tendo em vista as noções do ciberespaço como domínio, Libicki (2012) caracteriza como uma doutrina de caráter enganosa e até prejudicial, pois diante do

questionamento se o ciberespaço pode ser considerado um domínio ou não, ainda não existe um número significativo de declarações a respeito da temática (LIBICKI, 2012)

3.2 O Espaço Cibernético na perspectiva da China, Rússia e Coreia do Norte

Entre os anos 2013 à 2015, o Diretor de Inteligência Nacional, James R. Clapper, foi responsável por nomear a ameaça cibernética como o a ameaça estratégica número um aos Estados Unidos, colocando até na dianteira do terrorismo pela primeira vez desde os ataques de 11 de Setembro de 2001. Após isso, potenciais adversárias estatais e não-estatais tem desenvolvido capacidades responsáveis de conduzirem ataques cibernéticos maliciosos contra os interesses dos Estados Unidos. Nessa esteira, é possível afirmar que vários são as razões em que atores podem penetrar os Estados Unidos, como o roubo de propriedade intelectual, interromper operações de organizações com fins ativistas e conduzir ataques destrutivos que podem alcançar objetivos militares (DEPARTMENT OF DEFENSE, 2015).

O Departamento de Defesa ainda afirma que progressivamente os adversários têm realizado investimentos em segmentos cibernético, como a Rússia, China e Coreia do Norte. Os russos têm desenvolvido algumas capacidades que podem ser difíceis para que os EUA consigam detectar suas reações intenções. Em relação aos chineses, é percebido que graças às capacidades e estratégias avançadas, a China tem roubado propriedade intelectual de empresas globais para beneficiar empresas chinesas na competitividade com os EUA. A Coreia do Norte tem capacidades cibernéticas menos desenvolvidas, mesmo assim tem demonstrado certo nível de intenção hostil para com os Estados Unidos e seus interesses no ciberespaço (DEPARTAMENT DE DEFENSE, 2015).

3.2.1. China

Sobre as capacidades desenvolvidas no ciberespaço pela China, Brian M. Mazanec em sua obra *The Art of (Cyber War)* de 2009, elucida que a República Popular

da China (RPC), tem impulsionado cada vez mais o desenvolvimento de suas capacidades cibernéticas, não apenas focando na coleta de informação, mas também na capacidade de ocasionar danos econômicos, resultando danos na infraestrutura de seus adversários. A China está interessada em assuntos relacionados a guerra cibernética porque pode ampliar seu poder nacional, ou seja, o que pode ser entendido por Washington como uma ameaça para os Estados Unidos. Em *reports* recentes do Congresso americano a respeito do poderio da China, o Pentágono nota uma expansão de capacidades no domínio cibernético, o que desperta a procura de um melhor entendimento na estratégia de guerra cibernética chinesa (MAZANEC, 2009).

Nessa medida, Mazanec (2009) aponta que o foco contemporâneo da China em guerra cibernética é derivado de uma extensão de conceitos chineses como o do Sun Tzu que diz "superar o inferior com inferior" e do Mao Zedong "guerra do povo" estando ligado aos interesses geopolíticos do país como a sobrevivência do regime e a dominância na Ásia, como também a crescente influência a nível global.

A Guerra do Golfo foi um evento em que despertou o interesse da China nos assuntos relacionados à guerra cibernética. É evidenciado que os estrategistas chineses adotaram a RMA, e acreditavam que o futuro da guerra seria paulatinamente dependente da negação ou degradação do fluxo de informações do adversário. Os efeitos dessa decisão após uma década são bastante expressivos, e suas capacidades de atuar no ciberespaço foram ampliadas devido ao rápido crescimento econômico. Ademais, as capacidades cibernéticas chinesas tiveram crescimentos expressivos na promoção de defesa em redes de ataque e operações ofensivas contra adversários, como foi evidenciado por Richard Lawless, um subscretário Adjunto de Defesa para Ásia e Pacífico em 2007 (MANZANEC, 2009).

Segundo Clarke e Knake (2010), no que tange como a forma que os estrategistas chineses encararam as capacidades cibernéticas, pode-se afirmar que a doutrina de guerra assimétrica da China é baseada em um volume traduzido como *Guerra Irrestrita*, nesse livro publicado em 1999, tendo dois autores coronéis Qiao Liang e Wang Xiangsui (1999) do alto escalão do Exército Chinês afirma que países mais fracos podem vencer o status quo de potências maiores utilizado armas e táticas que estão fora do espectro tradicional militar. Ainda de acordo com os autores, a possibilidade de utilização de guerra cibernética contra uma força superior não significa diretamente que o país tenha intenção de lutar contra os Estados Unidos, mas sim que a nação deve se preparar para uma possibilidade eventual de conflito

Desde o final dos anos 1990, Clarke e Knake (2010) afirmam que a China tem apresentado características de uma nação que está criando uma capacidade ofensiva de guerra cibernética, desse modo tornando-se assim um possível alvo de adversários. Assim, o país criou uma série de medidas sobre o assunto. De acordo com os autores, as medidas estão expostas no quadro abaixo:

Tabela 3. Medidas tomadas pela China para a estratégica cibernética

1.	Criou um grupo de cidadãos hackers;
2.	Abrangeu espionagem cibernética, incluindo software e hardware de computadores dos EUA;
3.	Elaborou medidas necessárias para defender o seu próprio ciberespaço ;
4.	Unidades militares de guerra cibernética; e
5.	Um cerco à infraestrutura dos EUA com bombas-lógicas .

Fonte: Elaboração própria segundo Clarke e Knake (2010).

A China em seu desenvolvimento de sua estratégia cibernética, também fez o uso de *hackers* privados que são utilizados para dar suporte aos interesses do Estado. De acordo com a Comissão EUA-China para Segurança e Economia é relatado que existam 250 grupos de hackers que podem representar uma ameaça no ciberespaço para com os Estados Unidos. É destacado que a China utilizou seu ciberespaço pela primeira vez em forma de protesto em 1999, quando os Estados Unidos coordenou uma campanha área com a OTAN para parar os ataques vindos de forças sérvias contra o Kosovo. Devido ao mau uso de bombas lançadas pelos Estados Unidos no conflito, que deveriam ter sido lançadas sob a Diretoria Federal Iugoslava para Suprimento e Compras, acabaram acertando exatamente a embaixada chinesa. Diante disso, foi realizado uma série de protestos em frente as embaixadas-norte americanas que ansiavam por uma compensação as famílias e vítimas chinesas. Logo após o bombardeio, as páginas de web dos EUA e da OTAN foram focos de ataque de serviço de negação, como também agência dos governos terem suas caixas cheias de spam. Outro evento que pode ser apontado como uso do poder cibernético pelos hackitivistas foi quando um "avião espião" dos Estados Unidos entrou no espaço aéreo chinês em 2001, e esses cidadãos hackers chineses lançaram ataques de serviço de negação e *spam* (CLARKE; KNAKE, 2010).

Por conseguinte, em 2003, segundo Clarke e Knake (2010) a China anunciou a criação de unidades de guerra cibernética. As unidades estão situadas na ilha de Hainan e estão no Terceiro Departamento Técnico do Exército Popular de Libertação e as

Instalações de Inteligência de Sinais de Lingshui. Para o Pentágono, essas unidades têm como objetivo a defesa e o ataque no ciberespaço, e que também foram desenvolvidas armas cibernéticas de grande porte tecnológico e que são escassas a chances de projetar defesa. É conhecido ao menos 9 exemplos de tais armas e técnicas, como elucidadas no quadro abaixo:

Tabela 4. Armas e Técnicas Cibernéticas

1.	Instalação de minas de informação
2.	Realização de reconhecimento de informações
3.	Alteração de dados de rede
4.	Lançamento de bombas de informação
5.	Lançamento de informações lixo
6.	Aplicação de dissimulação de informações
7.	Divulgação de informações clonadas
8.	Organização de defesa da informação
9.	Estabelecimento de estações de redes espiãs

Fonte: Elaboração própria de acordo com Clarke e Knake (2010)

Com a permissão do governo Castro, a China estabeleceu duas "estações de espionagem de rede" em Cuba, durante o governo de Castro e assim os militares chineses foram responsáveis por um criar um serviço de monitoramento do tráfego de informações na Internet dos Estados Unidos, e outro também foi desenvolvido para monitorar as trocas de informações do Departamento de Defesa. Na mesma época em que era criado as unidades cibernéticas chinesas, coincidiu com um dos piores episódios de espionagem sofrida pelos Estados Unidos, conhecido como de Titan Rain, que se caracterizou como um ataque a rede do Pentágono que resultou na retirada de *terabytes* de informação. Os mesmos hackers também foram responsáveis por ataques a empresas de defesa como a Lockheed Martin e algumas instalações militares. Após uma série de investigação foi descoberto que os servidores intermediários eram localizados na Coreia do Sul e em Hong Kong, e no fim das investigações foi constatado que os servidores eram de Guandong, da China. Publicamente o Major General William Lord da Força Aérea dos Estados Unidos responsabilizaram os ataques sofridos ao Governo chinês (CLARKE e KNAKE, 2010).

A respeito do desenvolvimento de suas capacidades cibernéticas, é possível observar um maior investimento por parte dos líderes chineses. Como aponta, Manzec (2009), em 2003 o Exército Popular de Libertação foi responsável por organizar as primeiras unidades de guerra cibernética. E desde então a China, tem forçado

companhias de tecnologia de informação como a Microsoft a revelar sobre sensíveis propriedades de informações sobre os seus softwares e aplicações, desse modo, o Exército de Popular de Libertação utiliza as falhas de segurança, mais conhecidas como *dia zero (ZETA)* [17] , em aplicativos do Microsoft Office em explorar suas vulnerabilidades. Outrossim, também aumentam as chances da China plantar um software malicioso que pode ser responsável por obtenção de informações e também causar danos nas redes e infraestruturas.

De acordo o *report* Anual do Congresso norte-americano, *Military and Security Developments Involving the People's Republic of China* do ano de 2017, sobre as capacidades cibernéticas, é apresentado que nos anos recentes o Exército Popular de Libertação tem enfatizado uma maior importância no espaço cibernético como um novo domínio de segurança nacional e de área como competição estratégica. Com base no que foi apresentado pelo *white paper* da China de 2015, o país identificou o ciberespaço como um dos quatro "domínios críticos de segurança", ao lado dos marítimo, espacial e nuclear. Desta maneira, o Exército continua a desenvolver pesquisas a respeito do ciberespaço e de como podem explorar novas formas estratégicas no mesmo. Com o estabelecimento da Força de Suporte Estratégica, uma organização que foi estabelecida em 2015 e responsável por unir capacidades espaciais o espaço, cibernéticas e eletrônicas, pode ter representado um primeiro passo no desenvolvimento de forças cibernéticas e criar eficiências capazes para realizar os ataques e defesa da organização.

Nos escritos do Exército Popular de Libertação, o USCYBERCOM é considerado como uma referência de entidade consolidada única e de liderança simplificada. Visto isso, o Exército chinês reconhece os benefícios de uma liderança unificada e que possa estar centralizada na resolução e gestão de recursos cibernéticos, além de combinar suas capacidades ofensivas e defensivas sob uma organização militar. No mesmo *report,* é informado que nos escritos do Exército Popular de Libertação partem do princípio de dividir as operações cibernéticas entre períodos de guerra e período de paz. Em período de paz, as missões cibernéticas vão se comportar da maneira em que se deve defender o espaço eletromagnético e o ciberespaço, devido a crescente dependência da China na economia de informação. E durante em tempos de guerra, as capacidades cibernéticas devem ajudar o Exército a entender quais são os

[17] Dia Zero pode ser entendido quando um fabricante de *software* lança um produto que possui problema de segurança desconhecido tanto por ele quanto pelas empresas antivírus, desta forma essa falha é chamada de dia zero (AVAST, 2018).

motivos do inimigo e ajudar as tropas a combater em operações e garantir sucesso (DEPARTMENT OF DEFENSE, 2017).

Nessa perspectiva, é pertinente expor as capacidades do Exército Popular de Libertação que estão em desenvolvimento com base no *report*. A China continua a desenvolver capacidades de dissuadir, deter e anular possíveis intervenções. Acerca das operações de informações são tidas como um elemento fundamental para controlar habilidades no moderno espectro de batalha. Os autores do Exército citam essa capacidade como uma "informação de bloqueio ou "domínio da informação" como sendo um fator fundamental para definição de condições necessárias e conseguir a superioridade no ar e mar e terra também. O conceito de "bloqueio de informação" se faz presente através do emprego do militar e não militares instrumentos do poder de estado no campo de batalha, e que estão inclusos o ciberespaço e o espaço (DEPARTMENT OF DEFENSE, 2017).

Sendo assim, sobre as operações no ciberespaço em desenvolvimento, o *report* ressalta que

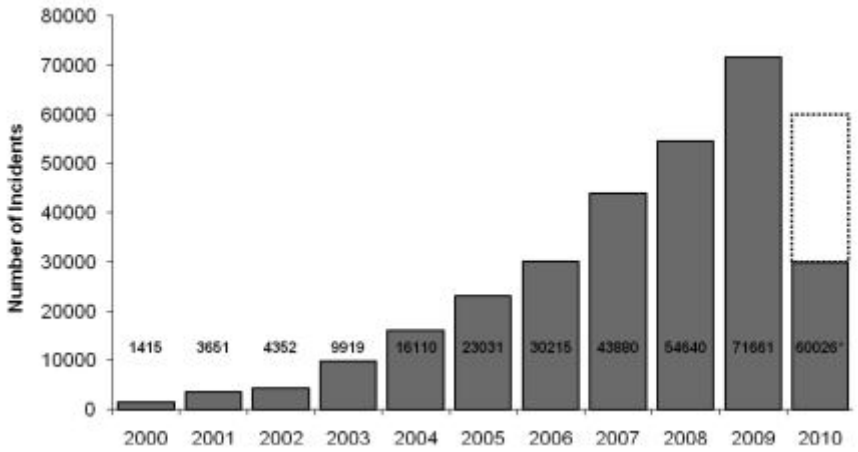
> China acredita que suas capacidades cibernéticas estão atrás dos Estados Unidos. Para lidar com essas deficiências, a China está melhorando seu treinamento e inovação para alcançar os seus objetivos relacionados ao desenvolvimento de capacidades cibernéticas. Pesquisadores do Exercito defendem a "superioridade do ciberespaço" usando operações cibernéticas ofensivas para deter ou interromper a capacidade do adversário de conduzir operações militares contra a China (DEFENSE OF DEPARTAMENT, 2017, p. 51-tradução nossa)

O Departamento de Defesa ainda afirma que o desenvolvimento das capacidades para com a guerra cibernética pelo Exército de Popular de Libertação identifica a guerra cibernética, eletrônica e psicológica como integrantes necessários para alcançar uma maior eficácia em combater o inimigo mais forte. No ano de 2016, o governo chinês identificou o ciberespaço como um domínio crítico para a segurança e logo declarou que iria acelerar o processo de desenvolvimento de suas forças cibernéticas. Nesse intento, com bases nos escritos do Exército Chinês pode-se afirmar que o mesmo utiliza suas capacidades de guerra cibernética para coletar dados com o propósito de inteligência e ataques cibernéticos, como também buscando restringir as investidas dos adversários em atividades baseadas na rede, comunicações e atividades comerciais (DEPARTMENT OF DEFENSE, 2017).

Nesse contexto, o Departamento de Defesa realiza um breve estudo das atividades cibernéticas direcionadas dos chineses contra o departamento. É visto que computadores de diversas partes do mundo têm sido alvos de ataques cibernéticos com origem da China, as intrusões se dão pelo acesso das redes e extração de informações. A nação chinesa usa de suas capacidades cibernéticas para recolher informações da diplomacia norte-americana, indústria de alta tecnologia, setores de base indústria e de defesa. As informações obtidas podem ser utilizadas em benefício de sua defesa em setores industriais como também dar suporte a modernização militar da China e promover uma série de informações ao Partido Comunista Chinês sobre o que se é planejado pelas lideranças norte-americanas. Diante disso, as informações coletadas podem servir como base para o Exército Popular de Libertação melhor organizar suas defesas em um possível combate com as redes dos EUA e outras capacidades que poderiam ser desenvolvidas para serem utilizadas em períodos de crise, isto é, acessos e habilidades são necessárias para que sejam utilizados na condução de ataques cibernéticos (DEPARTMENT OF DEFENSE, 2017).

Sendo assim, observando a figura abaixo, com base em dados no Departamento de Defesa, é demonstrado o volume de atividades maliciosas contra o próprio departamento na década passada e com projeções para 2010, vale salientar que nem todos os incidentes são derivados exclusivamente da China, pois o departamento ainda não possui esse nível de detalhamento em seus dados.

Tabela 5. Atividades Maliciosas Contra o Departamento de Defesa dos EUA



Fonte: *Report* do Congresso de 2010

Como pode ser observado a projeção de diminuição dos ataques para 2010, foi realizada com base na tomada de medidas que visam combater as ameaças cibernéticas, além de uma direção maior de recursos e estabelecimento do USCYBERCOM (DEPARTMENT OF DEFENSE, 2010).

Tendo em vista o que foi apresentado, é necessário que os Estados Unidos desempenhe cada vez mais esforços para fortalecer as capacidades do país no ciberespaço tanto de natureza ofensiva como defensiva. Desse modo, o Comando Estratégico pode desempenhar um papel fundamental como sincronizador para as operações no ciberespaço com o apoio da Força Tarefa de Operações em Redes Globais. De forma conjunta, o Comando junto com a Força Tarefa deve continuar a desenvolver capacidades de guerra cibernética para desabilitar a China em estágios iniciais de conflito, visto que há indícios que a nação chinesa aumentará sua sofisticação, severidade e investimentos como tecnologia cibernética. Em virtude disso, os Estados Unidos devem continuar com investimentos em suas capacidades cibernéticas, e assim preservar a segurança nacional e a liberdade norte-americana no domínio cibernético (MAZANEC, 2009).

No que tange assuntos relacionados a negociações de segurança cibernética, a China busca acordos internacionais que reduzam o risco político e segue em direção em a visões mais tradicionalistas de soberania nacional, em que aumenta a autoridade governamental sobre a Internet. Ainda, a China assume uma posição defensiva em discussões internacionais de normas de segurança cibernética, pois busca bloquear acordos que podem ser utilizados como justificativa contra as atuações chinesas no espaço cibernético (LEWIS, 2017).

3.2.2 Rússia

As autoridades de inteligência dos Estados Unidos consideram a Rússia como uma das maiores ameaças no ciberespaço, e os mesmos entendem que os russos possuem capacidades quase tão boas como os Estados Unidos (CLARKE; KNAKE, 2010).

A ascensão da Internet para centro da cultura e política russa ainda permanece pouco estudada (DEIBERT; ROHOZINSKI, 2010). Os autores ainda afirmam que devido ao fim da Guerra Fria e o fim da URSS, a Rússia os países que compõe a

Comunidade de Estados Independentes (CEI) entraram em um período de declínio. Devido a economias estagnadas, sistemas políticos em crise e a perda do status de superpotência logo fez com que as capacidades e avanço potencial fossem diminuídos.

Com o colapso da URSS, em 1991, o país apresentava a menor distribuição de linhas telefônicas entre os países industrializados. A capacidade de desenvolvimento científico da URSS, em especial no campo de computadores pessoais e redes de computadores era fraco para quase inexistente, pois a URSS não conseguiu desenvolver um número significativo de PCs, e a respeito das redes é possível destacar que foram pirateadas em engenharia de sistema reversos de outros países europeus (DEIBERT; ROHOZINSKI, 2010).

No entanto, a Rússia passou por um amplo processo de revolução de informação. De acordo com dados fornecidos pelo *Minitwatts Marketing Group*, em 2009, a respeito das estatísticas mundiais da internet, mais de 38 milhões de pessoas estavam online em solo russo, e a Rússia era o nono maior país em termos de usuários online no mundo (DEIBERT; ROHOZINSKI, 2010). Em dados atualizados de 2017, de acordo com a Conferência das Nações Unidas sobre Comércio e Desenvolvimento, o número de usuários da internet passou de 104 milhões, demonstrando assim um considerável crescimento nesses últimos anos.

A importância dos sistemas de informação aumentou consideravelmente na última década do século XXI, por causa do desenvolvimento da internet e a origem de novas informações e tecnologias de comunicação (DARCZEWSKA, 2016). Em 2000, foi adotada a Doutrina Militar da Federação Russa que simbolizou pela primeira vez que a segurança computadorizada necessitava de novos instrumentos e estratégias. Diferentemente das estratégias que eram adotadas pelas nações ocidentais, para os quais o ciberespaço era o contexto principal em considerar novos sistemas informatizados de combate e defesa. Desde o princípio os russos reconheceram a necessidade de suas forças armadas de operarem no "espaço de informação", como também reconheciam as ameaças enfrentadas pelo exército russo (DARCZEWSKA, 2016).

Adotada em setembro de 2000, a Doutrina de Segurança da Informação da Federação Russa, que ainda está vigorando atualmente, ressalta a importância da dimensão militar na questão da informação. Desse modo, a segurança de informação é vista como um fundamento para a segurança do Estado, pois é possível identificar as 'armas de informação' como instrumentos que possibilitam conseguir objetivos políticos (DARCZEWSKA, 2016). Além disso, a Doutrina identifica as principais

orientações em medidas relacionadas a defesa, tanto abordando aspectos tecnológicos e psicológicos. Entre os pensadores russos, existe uma dualidade na avaliação das ameaças de informações, visto que é citado as atividades tecnológicas estrangeiras ou conceitos de guerra de informação que são abordados por outros Estados. É possível ressaltar a preocupação que a Rússia tem em relações aos outros Estados, pois esses outros atores pretende conter os interesses da Rússia em campos informacionais (DARCZEWSKA, 2016)

O documento de Doutrina é um documento em que ainda se discute informações relacionadas as ameaças de informação e que afetam vários outros domínios (economia, política interna, ciência, tecnologia, defesa entre outros) além de introduzir termos utilizados em outros documentos oficiais e na ampla literatura popularizada incluindo noções de ‘guerra de informação’, ‘arma de informação’, e o ‘encobrimento da contra-ação de informação’ (DARCZEWSKA, 2016).

Darczewska (2016) ainda sobre a Doutrina de Segurança da Informação da Federação Russa que foi apresentada ao público e pretendia ser adotada no ano de 2016, releva a realização de tarefas específicas por parte do departamento de defesa no espaço de informação, menciona tarefas de longo prazo que devem continuar a monitorando as ameaças e desenvolver capacidades para melhor combatê-las. Desse modo, faz-se necessária a criação de condições visando o desenvolvimento de uma política militar de informação e contenção estratégica de conflitos no espaço de informação.

A respeito do papel do exército no espaço de informação, é observado que a Rússia diverge do modelo ocidental, visto que a noção do ciberespaço pelo modelo ocidental é vista mais com a noção apropriada no contexto militar. Enquanto os estrategistas russos utilizam a noção de ‘espaço de informação’ quando querem se referir a contextos de ameaças sociais, políticas e civilizacionais. Deste modo, seria uma forma de justificar as políticas internas e externas do *Kremlin*, no modo em que enfatizaria a natureza “informacional” das atividades do exército russo e não a sua natureza ‘cibernética’. Os estrategistas comportam-se de maneira que possam concentrar a informação e seu conteúdo, pois a missão confiada às Forças Armadas seria de neutralizar a influência das informações para seu próprio pessoal e sobre a população civil (DARCZEWSKA, 2016). Como um dos elementos que ocupam posição de destaque no pensamento estratégico militar é a noção de ‘Quarta Ameaça’. A tríade ocidental de ameaças cibernéticas conhecidas como guerra cibernética, terrorismo cibernético, crime cibernético foi expandida na Rússia para o que inclui a interferência

de informações nos assuntos dos Estados soberanos. Darczewska (2016) tendo base os princípios básicos para a política de Estado da Rússia em domínio de segurança informacional internacional para 2020, no que concerne o uso da tecnologia afirma que

> o uso da tecnologia da informação e comunicação como uma informação arma de informação para fins políticos e militares, com vista a interferir nos assuntos internos dos Estados, (…) minando a ordem pública, incitando a hostilidade racial ou religiosa, promovendo ideias e teorias racistas e xenófobas levando a ódio e discriminação e encorajando a violência (DARCZEWSKA, 2016, p. 15-tradução nossa).

No que tange a Quarta Ameaça, a Doutrina de Segurança da Informação Russa, postulada em 2000, afirmam que tal ameaça aparece na forma em que intimidam fatores da vida espiritual, isto é, representando um possível enfraquecimento da estabilidade social dos cidadãos. É observado que o uso de serviços estrangeiros nos meios de comunicação pode representar a disseminação da informação e a incapacidade da sociedade civil contemporânea russa de assegurar que os jovens absorvam valores éticos e patrióticos (DARCSEWSKA, 2016).

A Quarta ameaça apresenta uma dimensão prática, que serve de instrumento para objetivos políticos. Darczewska (2016) afirma que em 2000, a Quarta Ameaça teve importância na direção de ‘controlar negativas influências religiosas estrangeiras’. Em documentos doutrinários subsequentes as opiniões de especialistas militares viam a Quarta Ameaça como instrumento de oposição a uma técnica política utilizada pelos dos Estados Unidos e o avanço da OTAN (DARCZEWSKA, 2016).

Diante do contexto internacional, baseado no que é exposto pela Estratégia Nacional de Segurança da Rússia de 2015, é elaborado que a OTAN e os Estados Unidos desejam preservar seu protagonismo em assuntos globais. Darcsewka (2016) expõe que nos parágrafos 14 e 16 do documento, é demonstrada a noção de região euro-atlântica contra a região euroasiática, isto é, o contraste geopolítico da Eurásia com o conceito de Euro-Atlântico. Para melhor responder esse contraste, a Rússia almeja transformar a Organização de Tratado de Segurança Coletiva (OTSC), uma aliança militar intergovernamental, em uma organização internacional capaz de responder as ameaças políticas militares, e também ameaças estratégicas na esfera da informação (DARCZEWSKA, 2016).

Pode ser observado que a Rússia incentiva a produção de novas estratégias para

segurança nacional. Muita das vezes os conceitos e ideias desenvolvidas pelo país podem ser vistos como respostas a doutrinas ocidentais. Darczewska (2016) afirma que o conceito de informações no espaço pelas Forças Armadas Russas, publicadas em 2012, pode ser vista como uma resposta a publicação do documento de Defesa e Estratégia no Ciberespaço pelo Departamento de Defesa dos Estados Unidos, em 2011.

Tendo em consideração o que é exposto pelos documentos militares russos, pode-se afirmar que o país trata o espaço de informações de maneira similar da estratégia dos Estados Unidos lidam com o ciberespaço, reconhecendo como um novo campo estratégico operacional militar. Os documentos estratégicos russos diferentemente das estratégicas militares ocidentais partem do Presidente Putin, possuindo uma ampla estratégia de comunicação e são dirigidas a atores específicos, como na Rússia como no exterior. No campo interno, essa retórica anti-ocidental serve para promover seus interesses, como a demanda pelos cidadãos de um Estado forte e respeitado internacionalmente, isto é, representando uma maior mobilização da sociedade para com o a sensação de ameaça do Oeste (DARCZEWSKA, 2016).

Assim, a Rússia gradativamente tem buscado ampliar sua influência em sua vizinhança e além. Esse processo é realizado através de atividades como as Forças Armadas russas, que possuem estratégias de longo prazo no que tange o espaço de informação. Nesse intento, Darczewska (2016) expõe o envolvimento do exército em objetivos políticos-militares tem demonstrado posições mais radicais. A dissuasão psicológica é um dos elementos utilizados para aumentar a pressão sobre potenciais agressores. Transformações sucessivas em diversas doutrinas russas foram realizadas para espalhar o medo e aumentar a desconfiança do Ocidente.

Cada vez mais a Rússia em níveis operacionais tentará desenvolver instrumentos que possibilitem alcançar seus objetivos, incluindo medidas que visem ampliar o poder cibernético, defesa cibernética e capacidades ofensivas. Desse modo, será necessário que envolva uma maior coordenação de atividades entre vários atores na realização das mais variadas tarefas em nível operacional (DARCZEWSKA, 2016).

3.2.3 Coreia do Norte

A Coreia do Norte, oficialmente chamada de República Popular Democrática da Coreia (RPDC) é um dos países que possui a menor presença na internet do mundo.

Existe apenas cerca de 1024 IPs conhecidos em todo o país, que está em sua grande maioria sob o comando do governo. Em comparação com os Estados Unidos, existe cerca de 1,5 bilhões de IPs (PAGLIERY, 2014).

A RPDC possui uma intranet nacional chamada de *Kwangmyon*, que seria uma "pseudo-internet" disponível para os seus habitantes. Nesta intranet possui no máximo 5.500 sites em que os usuários acessam informações nas quais o governo norte-coreano autoriza seu acesso. Entretanto, é notável que o governo norte-coreano cada vez mais tem dedicado recursos significativos para o desenvolvimento de suas operações cibernéticas. Tendo em vista os governos que apresentam maior ameaça para os Estados Unidos, a RPDC é colocada na quarta posição, apenas atrás da China, Rússia e Irã (CONGRESSIONAL RESOURCE SERVICE, 2017).

Para melhor entender a política estratégica e suas capacidades cibernéticas, é necessário avaliar a balança estratégica na península coreana e além. Desde o fim da Guerra da Coreia (1950-1953), o principal objetivo do Exército Popular da Coreia é reunificar a Coreia sob a ordem da RPDC. Mesmo destinando uma grande parte do rendimento bruto nacional, uma guerra contra a Coreia do Sul soa como irrealista. Isso se deve ao fato da diminuição de recursos vindos da China e da Rússia, em contrapartida, os Estados Unidos ainda bem presença na Coreia do Sul (JUN; LAFOY; SOHN; 2015). Diante dessas circunstâncias, aparentemente é favorável manter uma vantagem na península coreana do que seguir com ações militares convencionais. Assim, a RPDC tem investido baixos investimentos se comparados com uma total modernização militar convencional, mas altamente efetivas como armas nucleares e mísseis balísticos. É elucidado também que a aquisição de capacidades de guerra irregulares assimétricas seria uma alternativa para RPDC. Dessa maneira a busca de capacidades militares irregulares e assimétricas vincula-se profundamente o desenvolvimento de recursos cibernéticos da RPDC. No caso norte-coreano, os ataques cibernéticos podem ser vistas como ferramentas provocativas devido a sua difícil retaliação e pode prejudicar seus oponentes a um custo baixo. Ações como crime, sabotagem, espionagem podem ser realizadas no ciberespaço, com o treinamento e infraestrutura operacional adequados (JUN; LAFOY; SOHN; 2015).

De acordo com o relatório intitulado de Serviço de Pesquisa do Congresso de 2015, no que tange a organização de operações cibernéticas norte-coreanas, é exposto que o regime de Kim são sediadas no Bureau Geral de Reconhecimento, mais especificamente o Bureau 121. O Bureau serve como uma espécie de central para que as

operações clandestinas da Coreia do Norte. Diante disso, o Exército Popular da Coreia tem como finalidade planejar as unidades cibernéticas e podem coordenar conjuntamente com Bureau. A Força Cibernética da Coreia do Norte foi estimada entre 3000 e 6000 hackers treinados em operações cibernéticas, sendo que a maiorias desses guerreiros pertencem ao Bureau e o *staff* do Exército Popular norte-coreano (JUN, LAFOY; SOHN; 2015).

Como é apontado por Jun, Lafoy e Sohn (2015), nos últimos anos a Coreia do Norte tem buscado aumentar seus ganhos financeiros e investir em operações cibernéticas, representando assim uma preocupação para experts em segurança dos Estados Unidos. Devido a testes nucleares realizadas pela Coreia do Norte, o Conselho das Nações Unidas tem realizado uma série de sanções contra o país. É notado que até mesmo a China que possui uma relação comercial de quase 80% com o país tem estado inclinado à pressionar o regime de Kim.

Desse modo, o uso de operações cibernéticas podem ser inseridas na estratégia nacional da Coreia do Norte em empregar forças e prejudicar seus adversários. Esses ataques podem ser configurados como uma perturbação do *status quo* com menor risco de retaliação (CONGRESSIONAL RESOURCE SERVICE, 2017). A respeito das unidades cibernéticas do Bureau Geral de Reconhecimento ainda se tem uma deficiência de literatura disponível em que relate como envolveu a sua origem, evolução e missão dessas unidades cibernéticas. Assim sendo, é difícil verificar a existências dessas operações que acontecem em níveis confidenciais (JUN, LAFOY e SOHN; 2015). A unidade cibernética mais importante é a Boreau 121, e sua gama de serviços incluem operações cibernéticas ofensivas e defensivas, espionagem cibernética, exploração de redes entre outros. De acordo com os autores, não existe um relatório de quem lidera o Bureau 101, mas tende-se a acreditar que sejam lideradas por Kim Yong Chol, o diretor geral do Boreau Geral de Reconhecimento.

Nesse contexto, Jun, Lafoy e Sohn (2015) relatam que como objetivos políticos emergentes, são vistas como recomendações ao menos quatro medidas que a aliança Estados Unidos-Coreia do Sul devem tomar para melhor gerenciar a emergência da ameaça norte-coreana no ciberespaço:

Tabela 6. Recomendações para Aliança EUA e Coreia do Sul

1.	“Preparar uma série de respostas diretas visando a Coreia do Norte como alvo”
2.	“Limitar a liberdade operacional da Coreia do Norte no”
3.	“Identificar e aproveitar as vulnerabilidades da Coreia do Norte para manter a

	balança estratégica”
4.	“Adotar medidas de mitigação e resilência de danos para garantir que os sistemas críticos de redes e resilência de danos estejam prontos para continuar com seu modo operacional mesmo após um ataque”

Fonte: Elaboração própria segundo Jun, Lafoy e Sohn (2015, p. 63-64).

Ainda no escopo de recomendações para os Estados Unidos conter as operações cibernéticas norte-coreanas, é incluído sanções que tem como alvo as informações de vulnerabilidade assimétricas e também pressionar por uma doação mais dura no que refere as relativas obrigações do Estado no ciberespaço. Os Estados Unidos deveriam considerar o desenvolvimento de políticas que possuíssem como foco os ataques cibernéticos de baixa intensidade e assim classificá-los como atos ilícitos. Possibilitando que a o nação norte-americana possa responder rapidamente e enviar um sinal claro como resposta a esses ataques, isto é, representando melhores efeitos dissuasivos. É apontado que medidas como a Ordem Executiva 13694 anunciada por 1º de abril de 2015, pelo presidente Barack Obama, evidenciam como os EUA devem estar preparados para responder crises futuras (JUN, LAFOY; SOHN; 2015).

Na resposta de ameaças no espaço cibernético contra os Estados Unidos, o USCYBERCOM quanto a NSA e Serviço de Segurança Central estão tomando medidas para desenvolver capacidades no ciberespaço de acordo com as orientações do Presidente. Em carta, do Comandante do USCYBERCOM para o Senador John McCain, em 2012, ao elucidar sobre o que seria necessário para defender os Estados Unidos de ataques cibernéticos originados da China ou Rússia, o comandante elucida que se faz necessário uma legislação em áreas como o compartilhamento de informações e fortalecimento da estrutural. Desse modo, a legislação representaria uma ferramenta que possibilitaria a diminuição de barreiras e falta de incentivos existentes que impedem que os responsáveis de compartilhar indicadores de ameaças cibernéticas com o governo (DEPARTMENT OF DEFENSE, 2012).

3.3 Desafios e perspectivas futuras do USCYBERCOM

Devido à natureza global das operações no domínio cibernético, é notório o surgimento de desafios para o Departamento de Defesa. As capacidades de combate

norte-americanas estão ligadas diretamente com esse domínio, o que requer um maior esforço na aquisição de alta tecnologia e capacidade operacional eficaz a qualquer momento (DEPARTMENT OF DEFENSE, 2016). Com o intuito de considerar os desafios recentes do USCYBERCOM, sob a óptica de general da Força Aérea Charles L. Moore Jr pode-se observar os desafios em combater o Estado Islâmico do Iraque e do Levante, pois o domínio cibernético é um ambiente em que se tem uma fácil adesão e de custo baixo, o que dificulta o reconhecimento do ponto de partida do ataque. No que tange a forma que o USCYBERCOM tem operado neste problema, é possível analisar a forma que o comando desafia este adversário e ainda podem assimilar diversas formas de construir uma base sólida e eficaz visando ao aproveitamento das operações. Mesmo reconhecendo o enfrentamento do USCYBERCOM em relação ao Estado Islâmico do Iraque e do Levante, Moore no comitê reconhece que existem outras ameaças no ciberespaço que devem ser observadas, e para que isso aconteça uma equipe estaria trabalhando em colaboração com o CYBERCOM e assim dar apoio as operações do comando em escala global (DEPARTMENT OF DEFENSE, 2016).

Ainda sobre os desafios existentes enfrentados pelo USCYBERCOM, foi realizado no dia 15 de novembro de 2017, no Forte de Meade em Maryiland, o primeiro *industry day* do USCYBERCOM que se reuniram em pró dos desafios apresentados pelo comando. O Comandante do USCYBERCOM destacou que os responsáveis deveriam ser "excelentes" e que deveriam ser ágeis na execução de programas. Salientou que os Estados Unidos não pode continuar protegendo suas capacidades de forma '*firehose*'[18], mas que devem ser mais precisos e diretos na abordagem. Rogers junto com o diretor do Grupo de Desenvolvimento de Capacidades do USCYBERCOM, Dennis Bartko voltaram a afirmar que parcerias são importantes para superar os desafios no domínio cibernético, e para isso era necessário uma partilha de informações com a indústria e que assim facilitaria o trabalho da Força Missão Cibernética. Bartko ainda comunicou que o Comando conseguiu autoridade pelo Congresso de ações avaliadas em 75 milhões de dólares por ano até Setembro de 2021, no intuito de desenvolver aparato e outros serviços em operações no ciberespaço. Segundo o diretor, o modelo de operações adotado é o DEVOPS, ou seja, um modelo é conhecido por limitar o tempo entre o conceito e implementação, permitindo que aconteça algumas mudanças caso

[18] Metáfora que significa "mangueira de incêndio", em que pode ser explicada quando há um envio muito rápido de informações de um computador de origem pra um computador destinatário e este tem que lidar com esse volume de informações.

necessárias (DEPARTMENT OF DEFENSE, 2017).

Sobre aspectos futuros do USCYBERCOM, o Comandante Rodgers, em San Diego do ano passado, discutiu o futuro do comando do Comando nos próximos 5 à 10 anos, ressaltando a importância à curto prazo de elevar o Comando Cibernético a um comando combatente. Outrossim, Rodgers demonstrou que gostaria que o comando integrado de forma ofensiva e defensiva, de um nível tático operacional. Em consequência disso, segundo o mesmo, o Comando poderia estabelecer um ambiente propício para que os tomadores de decisão sintam-se a vontade com as atividades cibernéticas em um nível tático.

No que tange a composição do USCYBERCOM, é possível afirmar que 80% é formado pelas forças armadas e 20% são civis, dessa maneira o Comando têm procurado atrair mais indivíduos que estejam interessado em atuar. O almirante ressalta que é importante a transmissão de uma auto-imagem para que esta força de trabalho se identifique com os "guerreiros digitais do século XXI", em que o indivíduo possa se enxergar como fundamental e inovador de extrema importância para o futuro. Tal atitude pode ser evidenciada no discurso

> as pessoas adoram falar sobre a tecnologia, mas nossa maior vantagem não é tecnologia; Nossa maior vantagem é que o homem motivado ou mulher com a capacidade intelectual de antecipar, ser inovador e ser ágil. Porque… estamos lidando com um homem ou uma mulher em algum lugar do mundo sentado em um teclado. Há uma dimensão humana em tudo isso. Não é apenas sobre a máquina (DEPARTMENT OF DEFENSE, 2017, tradução nossa).

No campo ofensivo, Rodgers reflete que quase desenvolvimento foi realizado de forma interna, mas que na aplicação de força cinética, ou seja, armas, recorrendo assim ao setor privado. De forma pessoal reflexiva, e o almirante tem dúvidas se esse é um modelo sustentável em longo prazo e questiona se assim estaria conseguindo o total empenho por parte do setor privado no desempenho de atividades cibernéticas (DEPARTMENT OF DEFENSE, 2017).

CONSIDERAÇÕES FINAIS

A presente monografia buscou analisar a inserção do ciberespaço quanto aos alcances estratégicos e político-militares dos Estados Unidos, em considerar o ciberespaço como um domínio operacional. Para isso, foi necessária uma elucidação de conceitos essenciais de assuntos relacionadas à revolução da informação que possibilitou o desenvolvimento de controles e comandos militares capazes de operacional no domínio cibernético.

Foi evidenciado conceitos importantes relacionados à informação, e como a mesma foi uma ferramenta utilizada no processo de comunicação e transformações de informações, comprovando organizações, sociedades e atores internacionais foram beneficiados pela revolução da informação, já que representou o aperfeiçoamento de tarefas como também um melhor ganho nas atividades que são desempenhadas. No caso dos Estados Unidos, o DARPA foi uma agência fundamental em promover a criação e desenvolvimento de novas tecnologias que fornecessem suporte às capacidades defensivas norte-americanas. É plausível ressaltar a importância da Guerra do Golfo em convergência com a RMA, pois foi um evento em que os EUA utilizaram um grande volume de armas com tecnologia de ponta e também a progressiva mudança do campo de batalha físico para o virtual. Cada vez mais os Estados têm destacado a importância de regulamentação do espaço cibernético, pois com a era da informação as redes e o processamento de dados desempenham papéis importantes em políticas estratégicas, não apenas nos EUA, mas também em outros países. Com a era digital e a disseminação da informação e comunicação na contemporaneidade trouxe desafios no que tange a elaboração de políticas nacionais e internacionais para melhor explicar o fenômeno da guerra cibernética. Esse tipo de guerra tem sido cada vez mais utilizada por Estados e atores não estatais para invadir computadores e redes com o intuito de causar danos e transtornos.

Além disso, devido à tecnologia de digitalização das redes militares, representou uma mudança de como os EUA defendia suas redes. É demonstrado que o USCYBERCOM é um comando operacional que possibilita a defesa e liberdade de atuação dos Estados Unidos e seus aliados e negação de atividades adversárias no ciberespaço. O comando também é responsável por fornecer treinamento especializado em questões no domínio cibernético e assim aumenta as chances de sucesso em suas missões. Vale ressaltar que o USCYBERCOM demonstra que a parceria a indústria

privada possui importância, pois a Guarda Cibernética foi bastante beneficiada em aspectos de treinamento devido a essa parceria. Diante das agências de ramos das Forças Armadas, a AFCYBER trabalha em conjunto com o USCYBERCOM em relação ao comando e controle de forças cibernéticas. Já a MARFOCYBER se alia no USCYBERCOM na perspectiva de melhor preparar equipes na Força Missão Cibernética. A outro ramo ARCYBER, é também um componente de suporte ao USCYBERCOM. Tendo em vista o que foi apresentado, a organização institucional é um fator primordial para que os EUA possam exercer capacidades combatentes no ciberespaço.

Devido à emergência de atores estatais no contexto internacional, cada vez mais os EUA tem enfrentado ameaças no que se refere ao domínio cibernético. China, Rússia e Coreia são os principais adversários nesse ambiente operacional; a China tem se organizado para melhor impulsionar suas capacidades cibernéticas. Como evento primordial que despertasse o interesse chinês em assuntos relacionados ao cyber, a China observou a forma com que os EUA conduziu a Guerra do Golfo, o que apresentou uma mudança militar-estratégica por parte da potência chinesa. Com o maior investimento por parte da China para com o ciberespaço como domínio combatente, o Exército Popular de Libertação é o responsável por criar unidades de guerra cibernética. É notado também que durante a última década, a China aumentou consideravelmente suas atividades contra o Departamento de Defesa norte-americano. A Rússia é outra nação que tem representado ameaças cibernéticas aos Estados Unidos. O país tem formulado doutrinas que possibilitam o desenvolvimento militar-tecnológico na questão de informação, como a Doutrina de Segurança da Informação. Mesmo com o expressivo desenvolvimento no campo cibernético o país tende buscar uma maior coordenação de atividades, e assim possa alcançar seus objetivos no cenário nacional, evitando influências externas, e no internacional. A Coreia do Norte é um ator que cada vez mais tem ganhando evidencia por buscar seus ganhos financeiros através do ciberespaço. Foi evidenciado que a Coreia do Norte utiliza de suas capacidades cibernéticas para perturbar o *status quo* dos adversários. Ainda não foram realizados estudos suficientes das operações norte-coreanas, visto que acontecem em níveis confidenciais e assim difícil de serem analisadas por estudiosos e acadêmicos da área cibernética. Como alternativa, a aliança dos Estados Unidos-Coreia do Sul é vista como primordial para melhor gerenciar as possíveis ameaças advindas da Coréia do Norte.

Foi apontado críticas ao USCYBERCOM, como o estabelecimento de uma

Força Cibernética independente, poderia representar uma melhoria nos serviços operacionais do comando, proporcionando assim uma maior capacidade de se organizar dentro do ambiente cibernético além de evitar desperdício de custos.

Tendo em vista o que foi apresentado, os Estados Unidos consideram o ciberespaço como um domínio operacional devido a emergência de ameaças por parte de atores estatais e não estatais no cenário internacional. Recentemente, ano de 2017, o USCYBERCOM foi elevado para Comando Combatente Unificado, representando assim uma maior autonomia de atuação. É necessário que continue o fluxo investimentos para esta unidade combatente, e assim possam desenvolver e criar novas capacidades cibernéticas de defender a nação no ciberespaço. A contratação e capacitação de combatentes é primordial para que propicie cenários de sucesso em suas futuras atuações. Vale destacar que o setor privado por meio de parcerias pode ser um aliado importante dos EUA, na capacitação e troca de informações que beneficiem a forma operacional. A formulação e atualização de doutrinas pelos Estados Unidos é essencial, já que o espaço cibernético está em constante mudança e isso requer esforço militar para que seja supridas necessidades no domínio cibernético.

REFERÊNCIAS

ESTADOS UNIDOS DA AMÉRICA. **US Air Force. History of HQ Twenty-Fourth Air Force and 624th Operations Center**. AFCYBER, 2014. Disponível em: <http://www.afcyber.af.mil/Portals/11/documents/About_Us/AFD-140429-035.pdf?ver=2016-04-26-113101-810>. Acesso em: 20 mar. 2018.

ALEXANDER, K. B.; JAFFER, J. N.; BRUNET, J. S. Clear thinking about protecting the nation in the cyber domain. **The Cyber Defense Review**, v. 2, n. 1, 2016. Disponível em: <https://ironnetcyber.com/assets/pdf/CDRV2N1_Clear%20Thinking_Alexander_Jaffer_Brunet_032217.pdf>. Acesso em: 2 fev. 2018.

ALEXANDER, K. B. **UNITED STATES CYBER COMMAND.** Whashington, DC, U.S.A. Disponível em: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-068b.pdf>. Acesso em 19 de abril de 2018.

ARMY CYBER. **About army cyber command: the army's frontline of cyber warfare.** 2017. Disponível em: <https://www.goarmy.com/army-cyber/about-army-cyber-command.html>. Acesso em 03 de abril de 2018.

ARQUILLA, John; RONFELDT, David. Cyberwar is coming!. **Comparative Strategy**, v. 12, n. 2, Spring 1993, p. 141-165.

_____. A new epoch - and Spectrum - of conflict. In: _____ (Ed.). **Athena's camp**: preparing for conflict in the information age. Santa Monica, CA: RAND Corporation, 1997. Disponível em: <https://www.rand.org/pubs/monograph_reports/MR880.html>. Acesso em: 18 abr. 2018.

AVAST. **DIA ZERO.** Disponível em: https://www.avast.com/pt-br/c-zero-day**>.** Acesso em 15 de maio de 2018.

BOHN, Eduardo C.; NOTHEN, Maurício R. Considerações sobre o ciberespaço e sua inserção nos Estudos Estratégicos. In: GUEDES DE OLIVEIRA, M. A.; GAMA NETO, R. B.; VILAR-LOPES, G. (Org.). **Relações Internacionais Cibernéticas (CiberRI**): oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: Editora da UFPE, 2016.

CALVETY, Myriam Dunn. **Cyber-security and threat politics**: US efforts to secure the information age. Nova York: Routledge, 2008.

CEPIK, Marco; CANABARRO, Diego; BORNE, Thiago. Cyberwar: Clausewitzian encounters. **Space & Defense**, USAF Academy, v. 8, n. 1, p. 19-33, 2015. Disponível em: <http://professor.ufrgs.br/marcocepik/files/cepik__canabarro__borne_-_2015_-_cyberwar.pdf>. Acesso em: 24 maio 2018.

CHAPMAN, G. **An introduction to the Revolution in Military Affairs**. Austin: University of Texas at Austin, 2003. Disponível em:

<http://www.lincei.it/rapporti/amaldi/papers/XV-Chapman.pdf>. Acesso em: 8 jan. 2018.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport, 2015.

CONGRESSIONAL RESEARCH SERVICE. **North Korean cyber capabilities: In Brief.** USA**,** 2017. Disponível em: <https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations>. Acesso em 20 de abril de 2018.

DAVIS, Norman C. An information-based revolution in military affairs. **Strategic Review**, v. 24, n. 1, 1996. Disponível em: <https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch4.pdf>. Acesso em: 20 dez. 2017.

_____. An information-based Revolution in Military Affairs. In: ARQUILLA, John; RONFELDT, David (Ed.). **Athena's camp**: preparing for conflict in the information age. Santa Monica, CA: RAND Corporation, 1997.

DENNING, D. E. **Rethinking the cyber domain and deterrence.** USA: JFQ 77, 2° Quarter, 2015. Disponível em: <http://ndupress.ndu.edu/Media/News/Article/581864/rethinking-the-cyber-domain-and-deterrence/>. Acesso em 11 de maio de 2018.

DEPARTMENT OF DEFENSE. **All cyber mission force teams archieve initial operating capability.** Whashington, DC, USA, 2016. Disponível em: <https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/>. Acesso em 15 de março de 2018.

DARPA. **Strategic Plan**. 2007. Disponível em: <https://microwaves101.com/downloads/DAPPA2007StrategicPlan.pdf> Acesso em: 05 jan. 2018.

ESTADOS UNIDOS DA AMÉRICA. Department of Defense. Military and security developments involving the People's Republic of China. **Annual Report to Congress**. Washington, DC: DoD, 2017. Disponível em: <https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF> Acesso em: 10 mar. 2018.

PEREZ, Ignacio D. Cybercom commander discusses evolving cyber threats. **DoD News**, Washington, DC, 27 fev. 2018. Disponível em: <https://www.defense.gov/News/Article/Article/1452601/cybercom-commander-discusses-evolving-cyber-threats/>. Acesso em: 16 mar. 2018.

DEPARTMENT OF DEFENSE. **Cybercom Commander: Other Nations' cyberspace ops intensified.** Washington, DC, USA, 2016. Disponível em: <https://www.defense.gov/News/Article/Article/698054/cybercom-commander-other-nations-cyberspace-ops-intensified/>. Acesso em 15 de março de 2018.

DEPARTMENT OF DEFENSE. **Cybercom Challenges Industry: Be agile, precise.** Washington, DC, USA, 2017. Disponível em:

<https://www.defense.gov/News/Article/Article/698054/cybercom-commander-other-nations-cyberspace-ops-intensified/>. Acesso em 10 de abril de 2018.

DEPARTMENT OF DEFENSE. **Cybercom commander: Public-Private partnerships needed for cybersecurity.** Washington, DC, USA, 2016. Disponível em: <https://www.defense.gov/News/Article/Article/1006807/cybercom-commander-public-private-partnerships-needed-for-cybersecurity/>. Acesso em 22 de maio de 2018.

DEPARTMENT OF DEFENSE. **Cybercom Tops list of threats to U.S., diretor of National Intelligence says.** Washington, DC, USA, 2018. Disponível em: < https://www.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/utm_source/DEFCONNews/utm_medium/Website/>. Acesso em 10 de maio de 2018.

DEPARTMENT OF DEFENSE. **Rogers discusses near future of U.S. cyber command.** Washington, DC, USA, 2017. Disponível em: <https://www.defense.gov/News/Article/Article/1094167/rogers-discusses-near-future-of-us-cyber-command/>. Acesso em 10 de abril de 2018.

DEPARTMENT OF DEFENSE. **The Doc cyber strategy.** Washington, DC, USA, 2015. Disponível em: <https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>. Acesso em 13 de fevereiro de 2018.

DEPARTMENT OF DEFENSE. **U. S. Cyber Command.** Washington, DC, USA, 2010. Disponível em: <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf>. Acesso em 15 de março de 2018.

DEPARTMENT OF DEFENSE. **U. S. Military's cyber capabilities provide strength, challenges, offincial says.** Washington, DC, USA, 2016. Disponível em: <https://www.defense.gov/News/Article/Article/810009/us-militarys-cyber-capabilities-provide-strength-challenges-official-says/>. Acesso em 10 de abril de 2018.

DEPARTMENT OF DEFENSE. **Worldwide cyber threats.** Washington, DC**,** USA, 2015. Disponível em: < https://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf>. Acesso em 20 de maio de 2018.

DEPARTMENT OF DEFENSE. **DoD's Network Defense Headquarters Achieves Full Operational Capability.** Whashington, DC**,** USA, 2018. Disponível em: < https://www.defense.gov/News/Article/Article/1429130/dods-network-defense-headquarters-achieves-full-operational-capability/>. Acesso em 10 de março de 2018.

DEIBERT, R; ROHOZINKSI, R. **Control and Subversion in Russian Cyberspace** Disponível em<https://pdfs.semanticscholar.org/48b5/50fe0dc602ea7e0a9d4f8f395d9ede34ae66.pdf>. Acesso em: 15 de Março 2018.

FAHRENKRUG, D. T. Cyberspace defined. National Military Strategy for Cyberspace Operations. Air University. 2007. Disponível em:

http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm>. Acesso em: 2 fev. 2018.

FOLKS, R. L. **Network centric warfare in the age of cyberspace operations**. Carlisle, PA: US Army War College, 2011. Disponível em: <http://www.dtic.mil/dtic/tr/fulltext/u2/a547453.pdf>. Acesso em: 13 maio 2018.

FOXALL, A. **Putin's cyberwar: Russia's statecraft in the fifth domain.** Russia Studies Centre, Policy Paper, n. 9, 2016. Disponível em: < https://www.stratcomcoe.org/afoxall-putins-cyberwar-russias-statecraft-fifth-domain>. Acesso em 11 de maio de 2018.

DARCZEWSKA, J. **Russia's Armed forces On the Information War Front.** Centre For Eastern Studies 2016. Disponível em < https://www.stratcomcoe.org/download/file/fid/5895> Acesso em 05 março de 2018.

GARDNER, Hall. War and the media paradox. In: KARATZOGIANNI, Athina. **Cyber conflict and global politics**. London: Routledge, 2005.

GARTZKE, E. **The myth of cyberwar: bringing war on the internet back down to Earth.** California, U.S.A., 2013. Disponível em: < http://pages.ucsd.edu/~egartzke/papers/cyberwar_12062012.pdf>. Acesso em 18 de maio de 2018.

GRAHAM, M. U.S. Cyber Force: One war away. **Military Review**, Army Press, maio/jun. 2016. Disponível em: <http://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160630_art018.pdf>. Acesso em: 3 mar. 2018.

GOVERNMENT ACCOUNTABILITY OFFICE (2017). DEFENSE CYBERSECURITY. DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened Report to Congressional Committees. Disponível em: <https://www.gao.gov/products/GAO-17-512> Acesso: 02 fevereiro 2018.

HELMS, C. P. **The digital GCC: USCYBERCOM as a combatant command.** Alabama, U.S.A: Air University, 2015. Disponivel em: < http://www.dtic.mil/dtic/tr/fulltext/u2/1012758.pdf>. Acesso em 29 de abril de 2018.

INTEL. **50 Years of Moore's Law.** Disponível em: https://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html>. Acesso em 11 de maio de 2018.

JOHNSON, R. **Cyber guard exercise focuses on defensive cyberspace operations.** U.S. Army, 2012. Disponível em: < https://www.army.mil/article/85786/cyber_guard_exercise_focuses_on_defensive_cyberspace_operations>. Acesso em 25 de maio de 2018.

JUN, J.; LAFOY, S.; SOHN, E. **North Korea's cyber operations: strategy and responses.** USA: Center for strategic international studies, 2015. Disponível em: < https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations>. Acesso em 20 de abril de 2018.

KREPINEVITCH, A. F. **Cavalry to computer, the pattern of military revolutions**. Tallahassee, FL: General Reference Center Gold, 1994. Disponível em: <http://users.clas.ufl.edu/zselden/Course%20Readings/Krepinevitch.pdf>. Acesso em: 4 jan. 2018.

_____. **Cyber warfare: a "nuclear option"?** Washington, DC: Center of Strategic and Budgetary Assessments, 2012. Disponível em: <https://csbaonline.org/research/publications/cyber-warfare-a-nuclear-option>. Acesso em: 22 jan. 2018.

KUEHL, Daniel T. From cyberspace to cyberpower: defining to problem. In: KRAMER, Frankin D.; STARR, Stuart H.; WENTZ, Larry K. (Ed.). **Cyberpower and national security**. cap. 2, p. 24-42. Disponível em: <http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf>. Acesso em: 15 jan. 2018.

LANDER, M; MARKOFF, J. **Digital fears emerge after data siege in Estonia.** The New York Times, 2007. Disponível em:<https://www.nytimes.com/2007/05/29/technology/29estonia.html>. Acesso em 24 de fevereiro de 2018.

LEWIS, J. A. **China's information constrols, global media influence, and cyber warfare strategy.** U.S. China Security and Ecomnomic Review Commission, 2017. Disponível em: <https://www.uscc.gov/sites/default/files/James%20Lewis%20May%204th%202017%20USCC%20testimony.pdf>. Acesso em 30 de maio de 2018.

LIBICKI, M. C. Cyberspace is not a warfighting domain. **Journal of Law and Policy**, v. 8, n. 2, 2012. Disponível em: <http://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlpsoc8&div=17&id=&page=>. Acesso em: 12 fev. 2018.

LIEB, Brian J. **Operationalizing Army Cyber.** Strategic Reasearch Project. Philadelphia, PA. 2013. United States Army War College. Class of 2013.

LYNN III, William J. Defending a new domain: the Pentagon's cyberstrategy. **Foreign Affairs**, September/October 2010 Issue. Disponível em: <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>. Acesso em : 22 jan. 2018.

MARFORCYBER. **U.S. Marine corps forces, cyberspace command**. Marine Corps, 2018. Disponível em: <https://marinecorpsconceptsandprograms.com/organizations/operating-forces/us-marine-corps-forces-cyberspace-command-marforcyber>. Acesso em: 4 abr. 2018.

MARINE CORPS. **Network centric warfare: Na emerging Warfighting Capability.** Quantico, USA, 1998. Disponível em: <http://www.dtic.mil/dtic/tr/fulltext/u2/a529329.pdf>. Acesso em 22 de maio de 2018.

MAZANEC, Brian M. **The Art of (Cyber)**. 2009. Disponível em: <http://www.neweraassociates.com/downloads/art_of_cyber_war.pdf> Acesso 03 de Maio de 2018.

MOLANDER, R. C.; RIDDILE, A. S.; WILSON, P. A. **Strategic information warfare: a new face of war.** USA: RAND Corporation. Disponível em: < https://www.rand.org/pubs/monograph_reports/MR661/index2.html>. Acesso em 25 de maio de 2018.

NYE JR, Joseph S. Nuclear lessons for cyber security? **Stratregic Studies Quarterly**, Winter 2011. Disponível em: <https://dash.harvard.edu/bitstream/handle/1/8052146/nyenuclearlessons.pdf?sequence=1>. Acesso em: 18 dez. 2017.

_____. Guerra e paz no ciberespaço. **Estadão**, São Paulo, 15 abr. 2012. Disponível em: <https://internacional.estadao.com.br/noticias/geral,guerra-e-paz-no-ciberespaco-imp-,861242>. Acesso em: 24 fev. 2018.

OAKLEY, J. **Cyber warfare: China's strategy to dominate in cyber space.** Kansas, USA: Faculty the U.S. Army Command and General, 2011. Disponível em: <www.dtic.mil/get-tr-doc/pdf?AD=ADA547718>. Acesso em 13 de maio de 2018.

OTTIS, R. **Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective.** Academic Publishing Limite, 2008. Disponível em: <https://ccdcoe.org/multimedia/analysis-2007-cyber-attacks-against-estonia-information-warfare-perspective.html>. Acesso em 02 de março de 2018.

PAGLIERY, J. **A peek into North Korea's internet.** CNN TECH, 2014. Disponível em: <http://money.cnn.com/2014/12/22/technology/security/north-korean-internet/index.html>. Acesso em 12 de maio de 2018.

POMERLAU, M. **Here's how DoD organizes its cyber warriors.** USA: Fifth Domain, 2017. Disponível em: <https://www.fifthdomain.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/>. Acesso em 19 de maio de 2018.

PRESIDENTIAL DOCUMENTS. **Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.** Federal Register, v. 80, n. 63, 2015. Disponível em: <https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf>. Acesso em 10 de maio de 2018.

SLOAN, Elinor C. **Modern military strategy**: an introduction. Oxon, NY: Routledge, 2012.

SHELDON, J. B. Deciphering cyberpower: strategic purpose in peace and war. **Strategic Studies**, v. 5, issue 2, 2011. Disponível em: <http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-05_Issue-2/Sheldon.pdf>. Acesso em: 18 maio 2018.

THE CIPHER BRIEF. **North Korea as a cyber threat,** 2018. Disponível em: < https://www.thecipherbrief.com/north-korea-as-a-cyber-threat>. Acesso em 19 de abril de 2018.

U.S. ARMY. **Timeline of army cyber command.** Disponível em: <https://www.goarmy.com/army-cyber/timeline-of-army-cyber.html>. Acesso em 23 de maio de 2018.

U.S. STRATEGIC COMMAND. **History.** USA, 2017. Disponível em: http://www.stratcom.mil/About/History/>. Acesso em 26 de maio de 2018.

WHITE HOUSE, Infrastructure & Technology. **Statement by presidente Donald J. Trump on the elevation of cyber command**. 2017. Disponível em: < https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/>. Acesso em 04 de abril de 2018.

WILSON, Clay. Congressional Research Service.v**Information operations and cyberwar: capabilities and related policy issues.** USA, 2006. Disponível em: < https://fas.org/irp/crs/RL31787.pdf>. Acesso em 26 de maio de 2018.

WOGAMAN, Donald G. **Network Centric Warfare: an emerging warfighting capability**. 1998. Disponível em: <http://www.dtic.mil/dtic/tr/fulltext/u2/a529329.pdf>. Acesso em: 27 maio 2018.